STIC Search Report
EIC 2100

STIC Database Tracking Number:

TO:
Location: Cpk2 4y03
Art Unit : 2134
Monday, September 15, 2003

Case Serial Number: 09/403071

From: David Holloway
Location: EIC 2100
PK2-4B30
Phone: 308-7794

david.holloway@uspto.gov

Search Notes

Dear Examiner ,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

STIC EIC 2100
Search Request Form

Today's Date: 9/15/03

What date would you like to use to limit the search?
Priority Date: 2/13/98 Other:

Name Tongoc Tran
AU 2134 Examiner # 79999
Room # 4403 Phone 305-7690
Serial # 09/403,071

Format for Search Results (Circle One):
(PAPER) DISK EMAIL

Where have you searched so far?
(USP DWPI EPO JPO ACM) IBM TDB
(IEEE) INSPEC SPI Other

Is this a "Fast & Focused" Search Request? (Circle One) (YES) NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

Title: Digital AV Data Transmitting Unit, Digital AV Data receiving Unit, Digital AV Data Transceiving Syster and Medium.

A two way digital AV Data Transmitting & receiving system comprising:
- means for determining significance of Data,
- storage means for storing plurality of authentication & or encryption rules)
- Selecting means for selecting one type of rule accordance w/ a decision result in data significance determination.
- Transmitting ~~Accordance~~ performed authentication accordance w/ Selected authentication rule.

Both Transmitting & receiving system have the Same means as stated above.

STIC Searcher David Holloway Phone 308-7799
Date picked up 9-15-03 Date Completed 9-15-03

Search and Information Resource Administration

```
Set     Items   Description
S1      13248   MULTIMEDIA? OR VIDEO? OR AUDIO? OR AV OR SOUND? OR MUSIC? -
             OR FILM? OR AUDIO?
S2       8982   BROADCAST? OR MULTICAST? OR SEND? OR TRANSMIT? OR TRANSMIS-
             SION? OR STREAMING OR TELECAST?
S3       9918   RATING? OR IMPORTANCE? OR SIGNIFICANCE? OR WEIGH? OR SCORE?
             OR RANK? OR PRIORIT? OR IMPORTAN?
S4        195   S3(3N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
             HIERARCH? OR MULTIPL? OR PLURAL?)
S5      15984   SECUR? OR AUTHENTICAT? OR VERIF? OR ENCRYPT? OR CRYPTOG? OR
             RSA OR PGP OR ACCESS()CONTROL?
S6        866   S5(2N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
             HIERARCH? OR MULTIPL? OR PLURAL?)
S7          0   S1 AND S2 AND S4 AND S6
S8          1   (S1 OR S2) AND S4 AND S6
S9          0   S1 AND S2 AND S3 AND S6
S10        13   (S1 OR S2) AND S3 AND S6
S11         4   S10 NOT PY>1998
S12         4   S11 NOT PD>19980213
File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Aug
         (c)2003 Info.Sources Inc
```

. 8/5/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00078992 DOCUMENT TYPE: Review

PRODUCT NAMES: SGML (830183); HTML (835277)

TITLE: A Look At SGML
AUTHOR: McLachlan, Gordon
SOURCE: HP Professional, v9 n6 p48(2) Jun 1995
ISSN: 0986-145X
HOMEPAGE: http://www.hppro.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Standard Generalized Markup Language (SGML), an open vendor-neutral method for sharing electronic documents, allows users to structure, format, and place content in documents. Three **important hierarchical** categories apply to each document: a declaration (a header describing document formatting and SGML options), type definition (a map of individual document elements, such as a graphic or **video** clip), and instance (the collection of elements that make up a viewed document). The best known SGML documents may be World Wide Web pages created using a SGML subset, Hypertext Markup Language (HTML). Web browsers are SGML parsers that recognize HTML-coded documents. The power of SGML lies in its ability to use delimited data fields for such data as control **security levels** and addressing for e-mail. Documents can then be linked into a database management-type system for easier storage and retrieval.

COMPANY NAME: Vendor Independent (999999)
SPECIAL FEATURE: Program Listings
DESCRIPTORS: Authoring Systems; Electronic Publishing; HTML; Hypertext; SGML; Web Site Design
REVISION DATE: 20020830

```
Set     Items   Description
S1    7522945   MULTIMEDIA? OR VIDEO? OR AUDIO? OR AV OR SOUND? OR MUSIC? -
            OR FILM? OR AUDIO?
S2    5573331   BROADCAST? OR MULTICAST? OR SEND? OR TRANSMIT? OR TRANSMIS-
            SION? OR STREAMING OR TELECAST?
S3   10897060   RATING? OR IMPORTANCE? OR SIGNIFICANCE? OR WEIGH? OR SCORE?
            OR RANK? OR PRIORIT? OR IMPORTAN?
S4     221158   S3(3N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S5    8265118   SECUR? OR AUTHENTICAT? OR VERIF? OR ENCRYPT? OR CRYPTOG? OR
            RSA OR PGP OR ACCESS()CONTROL?
S6     142946   S5(2N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S7          8   S1(5N)S2(S)S4(S)S6
S8         85   (S1 OR S2)(S)S4(S)S6
S9         85   S7 OR S8
S10        52   RD (unique items)
S11        35   S10 NOT PY>1998
S12        30   S11 NOT PD=19980213:20000213
S13        30   S12 NOT PD=20000213:20030920
S14         3   S1(5N)S2(5N)S3(S)S6
S15         3   S14 NOT S9
?show files
File 275:Gale Group Computer DB(TM) 1983-2003/Sep 12
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/Sep 12
         (c) 2003 The Gale group
File  75:TGG Management Contents(R) 86-2003/Sep W1
         (c) 2003 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2003/Sep 12
         (c) 2003 The Gale Group
File  16:Gale Group PROMT(R) 1990-2003/Sep 12
         (c) 2003 The Gale Group
File 624:McGraw-Hill Publications 1985-2003/Sep 12
         (c) 2003 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2003/Sep W1
         (c) 2003 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2003/Aug
         (c) 2003 The HW Wilson Co
File 696:DIALOG Telecom. Newsletters 1995-2003/Sep 15
         (c) 2003 The Dialog Corp.
File 553:Wilson Bus. Abs. FullText 1982-2003/Aug
         (c) 2003 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Sep 15
         (c) 2003 The Gale Group
File 674:Computer News Fulltext 1989-2003/Sep W1
         (c) 2003 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2003/Sep 15
         (c) 2003 The Gale Group
File 369:New Scientist 1994-2003/Sep W1
         (c) 2003 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2003/Sep 15
         (c) 2003 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2003/Sep 12
         (c) 2003 ProQuest Info&Learning
File   9:Business & Industry(R) Jul/1994-2003/Sep 12
         (c) 2003 Resp. DB Svcs.
File  13:BAMP 2003/Aug W5
         (c) 2003 Resp. DB Svcs.
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 647:CMP  Computer Fulltext 1988-2003/Aug W4
         (c) 2003 CMP Media, LLC
```

File 98:General Sci Abs/Full-Text 1984-2003/Aug
(c) 2003 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2003/Sep 15
(c)2003 The Gale Group
File 634:San Jose Mercury Jun 1985-2003/Sep 13
(c) 2003 San Jose Mercury News

13/3,K/11 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

03305419 Supplier Number: 44564254 (USE FORMAT 7 FOR FULLTEXT)
SECURITY CONSCIOUS
UNIX News, p45
April, 1994
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 708

... and Help. To show the relative security of your system or network, STK uses system ' **Ratings** ' and ' **Security Levels** '. To check the system, STK runs one or more security modules on it. Each module...

...Morris 'worm' in the Unix Mail facility. If a module finds a potential problem, it **sends** a message to the report database.
These security messages are rated numerically to indicate the...

13/3,K/18 (Item 2 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

00467032
Xerox Corp, the latest public network entrant, aims to outmaneuver its rivals with advanced techniques and equipment.
Data Communications December, 1978 p. 15-18

... nodes, earth stations, leased-satellite capacity and cellular radio and frequency reuse techniques. XTEN's **transmission** path will go from a user station (operating at up to 256 kbit/sec) through an interface to a roof-top transceiver. **Transmission** is then made to a local (or city) node in the petitioned band frequency. Besides the standard store-and-forward service, which includes a 'transparent pipeline,' **priority** levels, **multiple** distribution, and **encryption** capabilities, XTEN will offer a teleconferencing facility, to include still-frame **video** , 2-way digitized voice, and 5-10 sec facsimile.

13/3,K/26 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

09332413 SUPPLIER NUMBER: 19161393 (USE FORMAT 7 OR 9 FOR FULL TEXT)
A question of symmetry? (encryption alternatives)
Hardy, Stephen M.
Journal of Electronic Defense, v20, n1, p42(4)
Jan, 1997
ISSN: 0192-429X LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2829 LINE COUNT: 00231

... that cannot be successfully contested by the message originator
* security context: an establishment of the **security level** at which a **transmission** is taking place - a particularly **important** function in **multilevel security** environments.(2)
Data integrity and sequence integrity can be incorporated into either symmetric or asymmetric...

```
Set     Items   Description
S1    3134171   MULTIMEDIA? OR VIDEO? OR AUDIO? OR AV OR SOUND? OR MUSIC? -
            OR FILM? OR AUDIO?
S2    2049788   BROADCAST? OR MULTICAST? OR SEND? OR TRANSMIT? OR TRANSMIS-
            SION? OR STREAMING OR TELECAST?
S3    4887409   RATING? OR IMPORTANCE? OR SIGNIFICANCE? OR WEIGH? OR SCORE?
            OR RANK? OR PRIORIT? OR IMPORTAN?
S4     102522   S3(3N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S5    1628969   SECUR? OR AUTHENTICAT? OR VERIF? OR ENCRYPT? OR CRYPTOG? OR
            RSA OR PGP OR ACCESS()CONTROL?
S6      15711   S5(2N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S7          0   S1 AND S2 AND S4 AND S6
S8          6   S1 AND S4 AND S6
S9         17   S2 AND S4 AND S6
S10         0   (CATV OR VOD OR PPV OR CABLE()TELEVISION OR VIDEO(N)DEMAND
            OR PAY()PER()VIEW) AND S4 AND S6
S11        23   S8 OR S9
S12        20   RD (unique items)
S13        12   S12 NOT PY>1998
S14        12   S13 NOT PD=19980213:20010213
S15        12   S14 NOT PD=20010213:20030920
File   8:Ei Compendex(R) 1970-2003/Sep W1
         (c) 2003 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2003/Aug
         (c) 2003 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2003/Jul 31
         (c) 2003, EBSCO Publishing
File  65:Inside Conferences 1993-2003/Sep W2
         (c) 2003 BLDSC all rts. reserv.
File   2:INSPEC 1969-2003/Sep W1
         (c) 2003 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2003/Sep W2
         (c)2003 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Sep 11
         (c) 2003 The Gale Group
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003, EBSCO Pub.
File   6:NTIS 1964-2003/Sep W2
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2003/Sep W1
         (c) 2003 INIST/CNRS
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Sep W1
         (c) 2003 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Aug
         (c) 2003 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2003/Aug W4
         (c) 2003 FIZ TECHNIK
```

15/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2003 Elsevier Eng. Info. Inc. All rts. reserv.

05050676 E.I. No: EIP98074264144
Title: 1 Mbs energy/security scalable encryption processor using adaptive width and supply
Author: Goodman, James; Chandrakasan, Anantha P.
Corporate Source: Massachusetts Inst of Technology, Cambridge, MA, USA
Conference Title: Proceedings of the 1998 IEEE 45th International Solid-State Circuits Conference, ISSCC
Conference Location: San Francisco, CA, USA Conference Date: 19980205-19980207
Sponsor: IEEE
E.I. Conference No.: 48558
Source: Digest of Technical Papers - IEEE International Solid-State Circuits Conference 1998. IEEE, Piscataway, NJ, USA,98CH36156. p 110-111, 422 PAPER FA 7.2
Publication Year: 1998
CODEN: DTPCDE ISSN: 0193-6530
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9808W4
Abstract: An energy-scalable encryption processor in which the **level** of **security** and energy consumed to encrypt a bit can be traded-off dynamically, based on demand. This processor is based on a variable-width quadratic residue generator (QRG). The QRG is a cryptographically-secure pseudo-random bit generator. Since **transmitted** data streams can often be partitioned into different **priority levels** , and energy-scalable processor ensures that important information is protected, while sacrificing some security for low priority data, to reduce total system energy. 2 Refs.
Descriptors: *Digital computers; Cryptography; Security of data; Computer architecture
Identifiers: Energy scalable encryption processors
Classification Codes:
722.4 (Digital Computers & Systems); 723.2 (Data Processing)
722 (Computer Hardware); 723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

15/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2003 Elsevier Eng. Info. Inc. All rts. reserv.

03850457 E.I. No: EIP94051276823
Title: Investigation of the throughput and delay performance of MP-CSMA/CD using an adaptive algorithm with 2 levels of priorities
Author: Siew, C.K.; Er, M.H.
Corporate Source: Nanyang Technological Univ, Singapore
Conference Title: Proceedings of the 1993 IEEE Region 10 Conference on Computer, Communication, Control and Power Engineering (TENCON '93). Part 1 (of 5)
Conference Location: Beijing, China Conference Date: 19931019-19931021
Sponsor: IEEE
E.I. Conference No.: 20220
Source: Proceedings of the 10th IEEE Region Conference on Computer, Communication, Control and Power Engineering Proc 1993 IEEE Reg 10 Conf Comput Commun Control Power Eng (TENCON '93) 1993. Publ by IEEE, IEEE Service Center, Piscataway, NJ, USA. p 492-495
Publication Year: 1993
ISBN: 0-7803-1233-3
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9406W2
Abstract: An approach of implementing two **levels** of **priorities** in an MP-CSMA/CD local area network is presented. Our method uses different probability of **transmission** for different priorities. Our simulation results show that it is possible to implement two **levels** of **priority** if the bus has 10 percent of high priority stations and the overall load does not exceed 0.5. (Author abstract) 3 Refs.
Descriptors: *Local area networks; Network protocols; Algorithms; Adaptive systems; Data communication systems; User interfaces; Communication channels (information theory); Telecommunication traffic; Telecommunication control; Packet switching
Identifiers: Throughput; Delay performance; MP-CSMA/CD local area network ; Adaptive algorithms; **Priority levels** ; Distributed **access control** protocol; Medium access control; Congestion control function
Classification Codes:
722.3 (Data Communication, Equipment & Techniques); 722.4 (Digital Computers & Systems); 723.1 (Computer Programming); 723.2 (Data Processing); 716.1 (Information & Communication Theory); 922.1 (Probability Theory)
722 (Computer Hardware); 723 (Computer Software); 716 (Radar, Radio & TV Electronic Equipment); 922 (Statistical Methods)
72 (COMPUTERS & DATA PROCESSING); 71 (ELECTRONICS & COMMUNICATIONS); 92 (ENGINEERING MATHEMATICS)

15/5/6 (Item 3 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online
(c) 2003 ProQuest Info&Learning. All rts. reserv.

1023241 ORDER NO: AAD88-22182
PERFORMANCE ANALYSIS FOR HIERARCHICAL **AND** PRIORITY **BASED METROPOLITAN AND LOCAL-AREA COMMUNICATION NETWORKS**
Author: TSAI, ZSE-HONG
Degree: PH.D.
Year: 1988
Corporate Source/Institution: UNIVERSITY OF CALIFORNIA, LOS ANGELES (0031)
CHAIR: IZHAK RUBIN
Source: VOLUME 49/07-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 2790. 211 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL
Descriptor Codes: 0544

In this dissertation, **hierarchical** and **priority** based local area and metropolitan area network systems are considered. The local area networks investigated are assigned to operate in accordance with a priority based polling protocol, as is the case for token ring and token bus local area networks. Priority TDMA schemes are investigated as well. Such protocols are highly useful in providing **multiple - access control** for high speed integrated-services local and metropolitan area networks. In studying metropolitan area networks, we assume such systems to cover large geographical areas. We also assume that a wide-band **broadcast** (or repeater-based) communication channel is available, and is to be shared among a large number of users. We investigate the delay throughput performance of such metropolitan area networks, when double-tier network architectures are employed, using a polling backbone. Our performance results can be applied to the analysis and design of cellular radio networks, cable TV networks, optical-fiber networks, as well as a multitude of priority based local area networks.

15/5/10 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2003 Inst for Sci Info. All rts. reserv.

02519392 Genuine Article#: LH713 Number of References: 20
Title: RECOVERY MANAGEMENT FOR MULTILEVEL SECURE DATABASE-SYSTEMS
Author(s): KANG IE; KEEFE TF
Corporate Source: PENN STATE UNIV,DEPT ELECT & COMP ENGN/UNIV PK//PA/16802
Journal: IFIP TRANSACTIONS A-COMPUTER SCIENCE AND TECHNOLOGY, 1993, V21, P 225-247
ISSN: 0926-5473
Language: ENGLISH Document Type: ARTICLE
Geographic Location: USA
Subfile: SciSearch
Journal Subject Category: COMPUTER APPLICATIONS & CYBERNETICS
Abstract: Transactions are vital for database management systems because they provide transparency to concurrency and failure. For this reason, concurrency control and recovery are **important** issues in **multilevel secure** transaction processing systems. This paper examines the security properties of database recovery management protocols. We adopt an analytical approach to the problem in the sense that given a system described by a protocol, we attempt to determine if it is secure, rather than show how the system could be constructed from secure components. This is essential because a protocol that is inherently insecure can have no secure implementation. We present a model for transaction processing systems and a corresponding security property based on noninterference and demonstrate that the property is composable. This allows us to consider the security of each subsystem in the transaction processing system independently. We also present a recovery protocol for multiversion schedulers and show that this protocol is both correct and secure. The behavior of the recovery protocol depends only on previous actions of the same transaction. For this reason, we believe an untrusted implementation of the recovery manager may be feasible.
Descriptors--Author Keywords: DATABASE MANAGEMENT SYSTEMS ; SECURITY AND PROTECTION
Identifiers--KeyWords Plus: PRINCIPLES
Research Fronts: 91-1456 002 (DISTRIBUTED SYSTEMS; REPLICATED DATA; BYZANTINE AGREEMENT; RELIABLE **MULTICAST** COMMUNICATION; PROTOCOL DESIGN)
Cited References:
DOD520028STD DEP DEF, 1985
BELL DE, 1976, MTR2997 MITR CORP TE
BERNSTEIN PA, 1987, CONCURRENCY CONTROL
COSTICH O, 1991, 5TH IFIP WG 11 3 WOR
EFFELSBERG W, 1984, V9, P560, ACM T DATABASE SYST
GOGUEN JA, 1984, P75, P S SECURITY PRIVACY
GREENBERG I, 1991, DISTRIBUTED DATABASE
HAERDER T, 1983, V15, P287, COMPUT SURV
HAIGH JT, 1987, V13, P141, IEEE T SOFTWARE ENG
JAJODIA S, 1990, P360, MAY P IEEE S RES SEC
KANG IE, 1992, TR92103 PENNS STAT U
KARGER PA, 1991, P52, 1991 P IEEE S RES SE
KEEFE TF, IN PRESS IEEE T KNOW
KEEFE TFE, 1990, P369, 1990 P IEEE S RES SE
MCCULLOUGH D, 1990, V16, P563, IEEE T SOFTWARE ENG
MILLEN JK, 1990, P84, 3 P COMP SEC F WORKS
OBRIEN RC, 1990, RADCTR90387 SEC COMP
PAPADIMITRIOU C, 1986, THEORY DATABASE CONC
WILLIAM R, 1989, V5, RADCTR89313 SRI INT
WITTBOLD JT, 1990, P144, 1990 P IEEE S RES SE

```
Set     Items   Description
S1    2001980   MULTIMEDIA? OR VIDEO? OR AUDIO? OR AV OR SOUND? OR MUSIC? -
            OR FILM? OR AUDIO?
S2    1894659   BROADCAST? OR MULTICAST? OR SEND? OR TRANSMIT? OR TRANSMIS-
            SION? OR STREAMING OR TELECAST?
S3    1355298   RATING? OR IMPORTANCE? OR SIGNIFICANCE? OR WEIGH? OR SCORE?
            OR RANK? OR RATE?
S4      26984   S3(3N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S5    1011722   SECUR? OR AUTHENTICAT? OR VERIF? OR ENCRYPT? OR CRYPTOG? OR
            RSA OR PGP OR ACCESS?
S6      24772   S5(3N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR TIER? OR
            HIERARCH? OR MULTIPL? OR PLURAL?)
S7         15   S1 AND S4 AND S6
S8        242   S6 AND S4
S9       1645   S6 AND S1
S10         7   S9 AND IC=G06F-011/30
S11         8   S8 AND IC=H04N?
S12        15   S10 OR S11
S13         9   S12 NOT S7
S14     14093   S5(N)(LEVEL? OR TIER? OR RANGE? OR MULTILEVEL? OR HIERARCH?
            OR MULTIPL? OR PLURAL? OR SEVERAL? OR MANY? OR ADDITIONAL?)
S15      6525   S2 AND S14
S16       734   S1 AND S14
S17       969   (S15 OR S16) AND S3
S18       101   (S15 OR S16) AND S4
S19         7   S18 AND IC=(G06F? OR H04N?)
S20       127   S2 AND S8
S21         7   S20 AND IC=(G06F-011? OR H04N?)
S22         6   (S21 OR S19) NOT (S13 OR S11 OR S10)
S23        13   S1(3N)S2(3N)S3 AND S6
S24        12   S23 NOT (S21 OR S19 OR S13 OR S11 OR S10)
S25      6926   S1(2N)(RATING? OR RANK? OR SIGNIFI? OR IMPORT? OR WEIGH? OR
            SCORE? OR CATEGOR? OR CLASSIF? OR JUDG?)
S26       365   S1(2N)(PRIORIT? OR IMPORTANC?)
S27       199   (S25 OR S26)(5N)S2
S28         2   S27 AND S14
S29         2   S27 AND S6
S30         9   S27 AND S5
S31         7   S30 NOT S29
S32       958   S1 AND S2 AND S3 AND S5
S33       321   S32 NOT (RATE?)
S34        49   S33 AND IC=H04N?
S35        47   S34 NOT (S23 OR S31 OR S28 OR S19 OR S13 OR S10 OR S11 OR -
            S7)
S36      6796   MC=(W01-A05 OR W02-F05A)
S37         3   S36 AND S35
S38     13185   PPV OR VOD OR PAY()PER()VIEW OR VIDEO(2N)DEMAND? OR CATV OR
            CABLE()TELEVISION?
S39       120   S38 AND S6
S40        33   S34 AND IC=H04N-007?
S41        30   S40 NOT S37
S42        64   S39 AND IC=H04N-007?
S43         9   S39 AND S36
S44        64   (S42 OR S43) NOT (S41 OR S23 OR S31 OR S28 OR S19 OR S10 OR
            S11 OR S7)
S45        64   S44 NOT S13
S46        38   S45 NOT AD=19980213:20010213
S47        34   S46 NOT AD=20010213:20030920
File 347:JAPIO Oct 1976-2003/May(Updated 030902)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200358
         (c) 2003  Thomson Derwent
```

47/5/31 (Item 30 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

007037050
WPI Acc No: 1987-037047/198705
XRPX Acc No: N87-028042

Dynamic audio scrambler for pay TV encoding system - modulates audio information with different offset signals to define different scrambling modes

Patent Assignee: ZENITH ELECTRONICS CORP (ZENI)
Inventor: FORBES R L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 4636853	A	19870113	US 83564973	A	19831221	198705	B

Priority Applications (No Type Date): US 83564973 A 19831221
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 4636853	A		9		

Abstract (Basic): US 4636853 A

The scrambler includes an all-pass filter and a 90 degree phase shift circuit for supplying balanced modulators with 90 degree phase displaced audio information and 90 degree phase displaced carriers derived from the horizontal line frequency of a television receiver for producing a single sideband, suppressed carrier audio spectrum. A number of offset frequencies are derived from the horizontal line frequency and are used to further modulate the resultant signal to produce a single sideband displaced audio spectrum.

A logic circuit selects the offset frequency (mode) in response to vertical interval signals, video inversion signals and audio tone or data signals. The final output is thus scrambled in different modes with different offset frequencies. A complementary unscrambling system is also described.

ADVANTAGE - High **level** of **security** .

1/4

Title Terms: DYNAMIC; AUDIO; SCRAMBLE; PAY; TELEVISION; ENCODE; SYSTEM; MODULATE; AUDIO; INFORMATION; OFFSET; SIGNAL; DEFINE; SCRAMBLE; MODE
Index Terms/Additional Words: **CATV** ; SUBSCRIBER
Derwent Class: W02
International Patent Class (Additional): H04M-001/70; **H04N-007/16**
File Segment: EPI

47/5/21 (Item 20 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

010492697
WPI Acc No: 1995-394017/199551
Related WPI Acc No: 2003-232108
XRPX Acc No: N95-287282

Crypt key distribution system for data-base or CATV access - links communications unit by telephone to control centre and transmits crypt key by multiplex broadcast to allow access to encoded information

Patent Assignee: MITSUBISHI CORP (MITS)
Inventor: MOMIKI S; SAITO M
Number of Countries: 005 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 676897	A2	19951011	EP 95103978	A	19950317	199551	B
JP 7283809	A	19951027	JP 9470643	A	19940408	199601	
EP 676897	A3	19961113				199701	
US 6097816	A	20000801	US 95418195	A	19950407	200039	
EP 676897	B1	20030604	EP 95103978	A	19950317	200344	
DE 69530955	E	20030710	DE 630955	A	19950317	200353	
			EP 95103978	A	19950317		

Priority Applications (No Type Date): JP 9470643 A 19940408
Cited Patents: 1.Jnl.Ref; EP 450841; JP 62169540; US 4736422; US 5144663; WO 8909528
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 676897	A2	E	17	H04N-007/167	
Designated States (Regional): DE FR GB					
JP 7283809	A		9	H04L-009/06	
US 6097816	A			H04L-009/00	
EP 676897	B1	E		H04N-007/167	
Designated States (Regional): DE FR GB					
DE 69530955	E			H04N-007/167	Based on patent EP 676897

Abstract (Basic): EP 676897 A

The data-base access or **CATV** system includes crypt keys to permit access to the information. The system has a broadcast station transmitting over a multiplex broadcasting system. A **CATV** charging centre provides **CATV** signals and performs charging. A receiving unit is linked to the charging centre via a telephone line. It is also linked to a display via on or off-line links.

The charging station provides a viewing permit code including descrambling codes via the broadcast station and the receiver passes it to the display.

ADVANTAGE - Supplying crypt keys even when there are many requests.

Dwg.0/14

Title Terms: CRYPT; KEY; DISTRIBUTE; SYSTEM; DATA; BASE; **CATV** ; ACCESS; LINK; COMMUNICATE; UNIT; TELEPHONE; CONTROL; CENTRE; TRANSMIT; CRYPT; KEY ; MULTIPLEX; BROADCAST; ALLOW; ACCESS; ENCODE; INFORMATION
Derwent Class: T01; W01; W02
International Patent Class (Main): H04L-009/00; H04L-009/06; **H04N-007/167**
International Patent Class (Additional): H04K-001/00; H04L-009/14; **H04N-007/16**
File Segment: EPI

47/5/18 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

010691746 **Image available**
WPI Acc No: 1996-188702/199619
XRPX Acc No: N96-157796

Tiered bandwidth expansion and remote authorisation function for cable television **system - generating tier-control signal to allow subscriber to receive high-band tier and to allow prevent cable operator from denying specific tier to any customer with appropriate channel expander box**

Patent Assignee: ASIAN TELEVISION & COMMUNICATIONS INT LL (ASTE-N)
Inventor: BASAWAPATNA G R; BASAWAPATNA V; SIE J J; BASAWAPATNA G

Number of Countries: 060 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9609723	A1	19960328	WO 95US11304	A	19950906	199619	B
AU 9535847	A	19960409	AU 9535847	A	19950906	199629	
CN 1161768	A	19971008	CN 95195258	A	19950906	200309	
			WO 95US11304	A	19950906		

Priority Applications (No Type Date): US 94308922 A 19940922
Cited Patents: GB 2089623; US 3882266; WO 9416527
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9609723	A1	E	19	H04N-007/16	

Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU JP KE KG KP KR KZ LK LR LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT KE LU MC MW NL OA PT SD SE SZ UG

AU 9535847	A	H04N-007/16	Based on patent WO 9609723
CN 1161768	A	H04N-007/16	Based on patent WO 9609723

Abstract (Basic): WO 9609723 A

The method for providing controlled **access** to a **tier** of television channels transmitted over a **cable television** system (300) involves providing an access control signal (101) for governing **access** to a protected **tier** of the television channels, and transmitting a television signal (310) which includes the access control signal over the **CATV** system.

The television signal is received at a subscriber site, and subscriber access is provided to all television channels in the protected **tier** only when the **access** control signal is detected in the television signal at the subscriber site.

ADVANTAGE - Provides **tiering** and **access security** for **CATV** systems having bandwidths of approximately 450 MHz or less and which do not use addressable converters or decoders. Inexpensive with two **levels** of **security** .

Dwg.1/3

Title Terms: TIER; BANDWIDTH; EXPAND; REMOTE; AUTHORISE; FUNCTION; CABLE; TELEVISION; SYSTEM; GENERATE; TIER; CONTROL; SIGNAL; ALLOW; SUBSCRIBER; RECEIVE; HIGH; BAND; TIER; ALLOW; PREVENT; CABLE; OPERATE; SPECIFIC; TIER ; CUSTOMER; APPROPRIATE; CHANNEL; EXPAND; BOX
Derwent Class: W02; W03
International Patent Class (Main): **H04N-007/16**
File Segment: EPI

41/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2003 JPO & JAPIO. All rts. reserv.

05609430 **Image available**
METHOD AND DEVICE FOR CONTROLLING **TRANSMISSION** OF PROGRAM RELATED INFORMATION

PUB. NO.: 09-224230 [JP 9224230 A]
PUBLISHED: August 26, 1997 (19970826)
INVENTOR(s): YAMAGISHI YASUAKI
APPLICANT(s): SONY CORP [000218] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-330990 [JP 96330990]
FILED: December 11, 1996 (19961211)
INTL CLASS: [6] **H04N-007/16** ; H04H-001/00; H04H-001/02; **H04N-007/08** ; **H04N-007/081**
JAPIO CLASS: 44.6 (COMMUNICATION -- Television); 44.5 (COMMUNICATION -- Radio **Broadcasting**)

ABSTRACT

PROBLEM TO BE SOLVED: To attain the **transmission** control of program related information predicting the **access** tendency of viewers in the future by collecting viewing history information obtained corresponding to the viewing operations of viewers and controlling the **transmission** conditions of program related information based on that information.

SOLUTION: Concerning an EPG system with which the program related information such as the titles, channels and time of multichannel **broadcasting** programs is displayed on a television monitor 115 of viewer, when the viewer selects a program by operating a remote controller 116 while displaying the EPG information, that viewing history is **transmitted** through a public telephone line network to a customer management system 102 together with charging information. Based on the collected information, a database center 101 instructs the improvement of density of the EPG information concerning a program with a high audience **rating** or a promotion program and **sends** that instruction to an up-link center 107 together with the EPG information and a **transmission** control signal, etc. The center 107 improves the **transmission** frequency of the designated EPG information, superimposes it on an **AV** data stream sent from a program supplier 109 and **transmits** it toward a satellite 112.

41/5/10 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

015478681 **Image available**
WPI Acc No: 2003-540828/200351
XRPX Acc No: N03-428931
Personalized channel provision method for television broadcast **system, involves displaying currently** broadcasted audio / video **file or previously stored file, based on content** rating **table**
Patent Assignee: BALOGH S P (BALO-I); BRIDGES B D (BRID-I); CONNELLY J H (CONN-I); TRAW B (TRAW-I)
Inventor: BALOGH S P; BRIDGES B D; CONNELLY J H; TRAW B
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030066090	A1	20030403	US 2001966676	A	20010928	200351	B

Priority Applications (No Type Date): US 2001966676 A 20010928
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030066090	A1		22	H04N-007/173	

Abstract (Basic): US 20030066090 A1
NOVELTY - The meta-data describing **audio / video** files currently **broadcasted** or to be **broadcast** by the server (103), is received. One of the currently **broadcast** files or a previously stored file described by the meta-data, is selected based on a content **rating** table generated responsive to previously **accessed** files. The selected data file is stored and displayed on a personalized channel.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(1) an apparatus for providing personalized channel; and
(2) a processor-readable medium storing program for providing personalized channel.
USE - For television **broadcast** system.
ADVANTAGE - The best stored **broadcast audio / video** file is automatically selected for display on the personalized channel, by using the content **rating** table that is based on a user's profile and viewing habits.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the **broadcast** system.
server (103)
pp; 22 DwgNo 1A/14
Title Terms: PERSON; CHANNEL; PROVISION; METHOD; TELEVISION; **BROADCAST** ; SYSTEM; DISPLAY; CURRENT; **AUDIO** ; **VIDEO** ; FILE; STORAGE; FILE; BASED; CONTENT; **RATING** ; TABLE
Derwent Class: T01; W02; W03
International Patent Class (Main): **H04N-007/173**
File Segment: EPI

41/5/11 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

015403537 **Image available**
WPI Acc No: 2003-465677/200344
Related WPI Acc No: 2000-389086
XRPX Acc No: N03-370363

Broadcast **programme processing method in cable TV, involves selecting parameter of desired programme based on its** broadcast **source, from equivalent parameters from different** broadcast **sources**

Patent Assignee: THOMSON LICENSING SA (CSFC)
Inventor: SCHNEIDEWEND D R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6529526	B1	20030304	US 9892616	P	19980713	200344	B
			US 98191056	A	19981112		

Priority Applications (No Type Date): US 9892616 P 19980713; US 98191056 A 19981112
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6529526	B1		13	H04N-007/50	Provisional application US 9892616

Abstract (Basic): US 6529526 B1

NOVELTY - Packetized programme information containing a equivalent programme specific parameters such as programme content **rating** , caption information and text descriptive information of a desired programme, are received from different **broadcast** sources. One of the received programme specific parameters is selected based on its **broadcast** sources, to process the desired programme.

USE - For processing **broadcast** programme in digital **video** and **audio broadcast** applications for terrestrial, cable TV (CATV), satellite, Internet or computer network systems.

ADVANTAGE - Selected programme specific parameter comprises content **rating** that is mapped to different programme content **rating** system and used in validating authorization to **access** the desired programme, hence erroneous display of invalid and objectionable images are prevented reliably.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the digital **video** receiver.

pp; 13 DwgNo 1/5

Title Terms: **BROADCAST** ; PROGRAMME; PROCESS; METHOD; CABLE; TELEVISION; SELECT; PARAMETER; PROGRAMME; BASED; **BROADCAST** ; SOURCE; EQUIVALENT; PARAMETER; **BROADCAST** ; SOURCE
Derwent Class: T01; W03
International Patent Class (Main): **H04N-007/50**
File Segment: EPI

41/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2003 JPO & JAPIO. All rts. reserv.

06976428 **Image available**
BROADCASTING AND PROJECTION CONTROL SYSTEM USING IC CARD

PUB. NO.: 2001-203999 [JP 2001203999 A]
PUBLISHED: July 27, 2001 (20010727)
INVENTOR(s): TAKANO ASAHARU
APPLICANT(s): DAINIPPON PRINTING CO LTD
APPL. NO.: 2000-010418 [JP 200010418]
FILED: January 19, 2000 (20000119)
INTL CLASS: **H04N-007/16**

ABSTRACT

PROBLEM TO BE SOLVED: To easily change the setting of **rating** information and also enable only limited viewers to change the **rating** information.

SOLUTION: When an IC card 5 which can be connected to a receiving projection device 2 and has set **authentication** information for confirming at least the bearer and **rating** information is connected to the receiving projection device 2, the projection of **video** sent from a program providing server 1 is controlled according to the **rating** information set on the IC card.
COPYRIGHT: (C)2001,JPO

24/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2003 JPO & JAPIO. All rts. reserv.

06473748 **Image available**
DIGITAL AV DATA TRANSMISSION UNIT, DIGITAL AV DATA RECEPTION UNIT, DIGITAL AV DATA TRANSMISSION/RECEPTION SYSTEM AND MEDIUM

PUB. NO.: 2000-059323 [JP 2000059323 A]
PUBLISHED: February 25, 2000 (20000225)
INVENTOR(s): NISHIMURA TAKUYA
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI
USUKI NAOJI
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD
APPL. NO.: 10-224825 [JP 98224825]
FILED: August 07, 1998 (19980807)
PRIORITY: 10-031847 [JP 9831847], JP (Japan), February 13, 1998 (19980213)
10-151586 [JP 98151586], JP (Japan), June 01, 1998 (19980601)
INTL CLASS: H04H-001/00; H04L-009/08; H04L-009/10; H04L-029/08; H04N-007/167

ABSTRACT

PROBLEM TO BE SOLVED: To appropriately perform data communication while being immune to forgery or alteration and considering the importance of data or class of a recognition method by receiving an authentication request and performing authentication based on one kind of authentication rule selected out of a means storing **plural authentication** rules on the side of transmission based on the discriminated result of a data importance discriminating means.

SOLUTION: When an authentication requesting means 12 receives the authentication request, a data **importance** discriminating means 3 discriminates the **importance** of **AV** data 2 to be **transmitted** and classifies them according to CGMS values. A transmission side authentication selecting means 6 sends the optimum authentication rule, which is selected out of a means 5 storing **plural authentication** rules on the side of transmission, to a digital AV reception unit TV9. At a digital AV transmission unit STB1, the same authentication rule as the selected certification rule is selected and a reception side authentication means 13 and a transmission side authentication means 7 mutually perform the authentication. When the authentication is made successful, the AV data 2 to be transmitted are enciphered and transmitted while using a work key Kco16 and the received enciphered data are deciphered by a work key Kco17.
COPYRIGHT: (C)2000,JPO

37/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

014043075 **Image available**
WPI Acc No: 2001-527288/200158
XRPX Acc No: N01-391340
Broadcasting **and projection control system controls projecting unit based on setting of default** rating **value in integrated circuit card recognized by projecting unit**
Patent Assignee: DAINIPPON PRINTING CO LTD (NIPQ)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001203999	A	20010727	JP 200010418	A	20000119	200158	B

Priority Applications (No Type Date): JP 200010418 A 20000119
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001203999	A		5	H04N-007/16	

Abstract (Basic): JP 2001203999 A
NOVELTY - A server (1) multiplexes **rating** information with a **video** signal. A projecting unit (2) receives and projects a **broadcast** program sent by the server and compares the multiplexed **rating** information with a preset value to set a default **rating** value to an integrated circuit (IC) card. A control unit controls the projecting unit based on set default value. The **authentication** and **rating** information for confirming the authorized owner, are set in the IC card and is recognized by the projecting unit.
USE - For controlling **broadcast** and projection of **video** signal using integrated circuit (IC) card.
ADVANTAGE - Prevents unauthorized changing of **rating** information, by children.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of **broadcasting** projection control system. (Drawing includes non-English language text).
Server (1)
Projecting unit (2)
pp; 5 DwgNo 1/7
Title Terms: **BROADCAST** ; PROJECT; CONTROL; SYSTEM; CONTROL; PROJECT; UNIT; BASED; SET; DEFAULT; **RATING** ; VALUE; INTEGRATE; CIRCUIT; CARD; PROJECT; UNIT
Derwent Class: W02
International Patent Class (Main): **H04N-007/16**
File Segment: EPI

24/5/10 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

012744616 **Image available**
WPI Acc No: 1999-550733/199946
XRPX Acc No: N99-407529

Digital audiovisual data transmitting unit

Patent Assignee: MATSUSHITA ELECTRIC IND CO LTD (MATU); MATSUSHITA DENKI SANGYO KK (MATU)
Inventor: GOTOH S; IITSUKA H; NISHIMURA T; TAKECHI H; USUKI N; YAMADA M
Number of Countries: 021 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9941910	A1	19990819	WO 99JP533	A	19990208	199946 B
EP 977436	A1	20000202	EP 99902852	A	19990208	200011
			WO 99JP533	A	19990208	
JP 2000059323	A	20000225	JP 98224825	A	19980807	200021
CN 1263669	A	20000816	CN 99800482	A	19990208	200055

Priority Applications (No Type Date): JP 98224825 A 19980807; JP 9831847 A 19980213; JP 98151586 A 19980601
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9941910	A1	J	90	H04N-007/16	
Designated States (National): CN US					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 977436	A1	E		H04N-007/16	Based on patent WO 9941910
Designated States (Regional): DE FR GB					
JP 2000059323	A		28	H04H-001/00	
CN 1263669	A			H04N-007/16	

Abstract (Basic): WO 9941910 A1

NOVELTY - Digital **AV** data **transmitting** unit includes data **importance** judging section for judging importance of digital AV data, etc.

DETAILED DESCRIPTION - Digital AV data transmitting unit includes data **importance** judging section for judging **importance** of digital **AV** data, **transmitting** -side **multiple authentication** rule storage section stored with **multiple** kinds of **authentication** rules, transmitting-side authentication selecting section for selecting one kind of rules from transmitting-side **multiple authentication** rule storage section, and transmitting-side authenticating section for carrying out authentication based on the selected authentication rules. A digital AV data receiving unit includes an authentication requesting section for making an authentication request, a receiving side **multiple authentication** rule storage section stored with the same authentication rules as those stored in the transmitting-side **multiple authentication** rule storage section, a receiving-side authentication selecting section for selecting the preset authentication rules selected by the transmitting-side authentication selecting section from the receiving-side **multiple authentication** rule storage section, and a receiving-side authenticating section for carrying out authentication based on the authentication rules selected on the receiving side.

INDEPENDENT CLAIMS are included for a digital AV data receiving unit, and a digital AV data transmitting-receiving unit.

USE - For transmitting digital AV data.

DESCRIPTION OF DRAWING(S) - The drawing shows a diagram to illustrate the digital audiovisual data transmitting and receiver units.

pp; 90 DwgNo 1/15

Title Terms: DIGITAL; AUDIOVISUAL; DATA; TRANSMIT; UNIT
Derwent Class: W01; W02
International Patent Class (Main): H04H-001/00; H04N-007/16
International Patent Class (Additional): H04L-009/00; H04L-009/08; H04L-009/10; H04L-029/08; H04N-007/167

File Segment: EPI

22/5/5 **(Item 4 from file: 350)**
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

008519905 **Image available**
WPI Acc No: 1991-023989/199104
XRPX Acc No: N91-018484

Security control method for distributed processing system - defines security ratings for communication between servers where no central controller exists

Patent Assignee: INT COMPUTERS LTD (INCM)
Inventor: MCVITIE D G
Number of Countries: 008 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 409397	A	19910123	EP 90306141	A	19900606	199104	B
AU 9059143	A	19910124				199111	
US 5012515	A	19910430	US 90537609	A	19900614	199119	
ZA 9004545	A	19910424				199121	
EP 409397	A3	19920422	EP 90306141	A	19900606	199329	
EP 409397	B1	19960904	EP 90306141	A	19900606	199640	
DE 69028362	E	19961010	DE 628362	A	19900606	199646	
			EP 90306141	A	19900606		

Priority Applications (No Type Date): GB 8916586 A 19890720
Cited Patents: NoSR.Pub; 2.Jnl.Ref
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 409397	B1	E	9	G06F-001/00	
Designated States (Regional): BE DE FR GB IT					
DE 69028362	E			G06F-001/00	Based on patent EP 409397

Abstract (Basic): EP 409397 A

A security rating has a number of factors, each with a set of values which describe conditions for connection to take place. Each server has a security rating of itself (R1), each other server (R2) and of each route (R3). If a security rating is omitted it is assumed that all factors and their values are possible for connection. An initiator specifies a required **security level** (LA2) from the logical intersection of its own rating (R1) and the responder (R2). If this is empty then connection is not possible, otherwise a further rating (LA3) is formed from the logical intersection of the previous rating (LA2) and the route rating (R3).

If rating R2 contains factors with only one value then the initiator does not trust security information with the responder. Otherwise a connection request is made containing the factors common to the ratings (r2) and (LA3).

ADVANTAGE - No single repository of information about **security levels** in system. (7pp Dwg.No.2/3)

Title Terms: SECURE; CONTROL; METHOD; DISTRIBUTE; PROCESS; SYSTEM; DEFINE; SECURE; RATING; COMMUNICATE; SERVE; NO; CENTRAL; CONTROL; EXIST
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/00**
International Patent Class (Additional): **G06F-001/00** ; **G06F-007/04** ; **G06F-013/14** ; **G06F-015/16** ; H04L-009/00
File Segment: EPI

13/5/7 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003 Thomson Derwent. All rts. reserv.

014189948 **Image available**
WPI Acc No: 2002-010645/200201
XRPX Acc No: N02-008900

User authentication system for online banking, acquires reusable user-defined policy to define protection level for accessing of accounts

Patent Assignee: BIONETRIX SYSTEMS CORP (BION-N)
Inventor: BAKSHI B S; HELMS D W; ROCHON A C; WALKER T J

Number of Countries: 094 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200171961	A1	20010927	WO 2001US9188	A	20010323	200201	B
AU 200143706	A	20011003	AU 200143706	A	20010323	200210	

Priority Applications (No Type Date): US 2000695060 A 20001025; US 2000191471 P 20000323
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200171961	A1	E	60	H04K-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200143706	A		H04K-001/00	Based on patent WO 200171961

Abstract (Basic): WO 200171961 A1

NOVELTY - An authentication controller (208) manages the acquired user-defined policy for the account and credentials which define the protection **level** to **access** the account. A user management component (207) stores the acquired result and organizes the policy and credentials so that the credentials are reused to authenticate another account. An authentication server (202) uses the user-defined policy to authenticate account.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for the user authentication method.

USE - For providing user authentication during provision of services or exchange of confidential information through Internet, during online banking and shopping, online stock-trading, personalized content website perusal, business-to-business and business-consumer-e-commerce transactions, etc., using smart cards, tokens, fingerprint scanners, **audio** /face recognition systems etc.

ADVANTAGE - Protects confidential information available on the Internet and provides effective authentication of the user to Internet accessible application and services by acquiring a user defined policy defining a protection **level** for **accessing** the account.

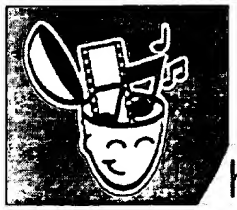
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of user authentication system.

Authentication server (202)
User management component (207)
Authentication controller (208)

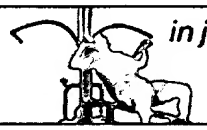
pp; 60 DwgNo 2/15

Title Terms: USER; AUTHENTICITY; SYSTEM; BANK; ACQUIRE; REUSE; USER; DEFINE ; DEFINE; PROTECT; LEVEL; ACCESS; ACCOUNT
Derwent Class: T01; W01; W02
International Patent Class (Main): H04K-001/00
International Patent Class (Additional): **G06F-011/30** ; G06F-015/16; G06F-017/60; H04L-009/00
File Segment: EPI

LYCOS ZONE™



howstuffworks

AD AD AD AD BOWFLEX delivers results  in just 6 GUAR

home Search

ComputerStuff AutoStuff ElectronicsStuff ScienceStuff HomeStuff EntertainmentStuff MoneyStuff TravelStu

Click here to go back to the normal view!

What does a V-chip really do and how does it work?

As of 1999, all new television sets (over 13 inches / 33 cm) sold in the United States have to contain a V-chip. The "V" stands for "**violence**," and the goal of the chip is to allow parents to choose the level of violent TV programming that will be allowed into the home.

The idea behind a V-chip is simple. TV shows have a signal embedded in them that gives the show a **rating**, and the chip can detect these ratings. The ratings that the FCC has settled on look like this:

- **TV-Y** - All children can watch; zero violence or sexual content
- **TV-Y7** - For children 7 and over
- **TV-G** - For general audiences; no sex, violence or inappropriate language
- **TV-PG** - Parental guidance suggested
- **TV-14** - Suitable only for people over 14; some sex or violence
- **TV-MA** - Suitable only for mature audiences; may contain graphic violence or sexual situations

A parent can **program** the TV with a rating, and the TV will **block** all shows above that rating. So if a parent programs in the TV-Y7 rating, the TV will allow shows rated at TV-Y and TV-Y7 but will block all other shows.

The ratings are encoded in what is called the "**line 21 data area**." If you have read the article How Television Works, then you know about the vertical retrace signal. This signal tells the TV to move the electron beam from the lower right to the upper left corner of the screen. Within this signal are horizontal retrace signals designed to keep the horizontal retrace circuit synchronized. The twenty-first line of horizontal retrace embedded within the vertical retrace area has been designated as a data area that is controlled by a standard called **XDS**. All sorts of things go inside this data area -- such as closed captioning information and the time of day -- as well as ratings information. See this page for details.

The V-chip simply **decodes** the line 21 data, **compares** it with the parent's allowed rating and then either blocks the signal or lets it through.

Here are some interesting links:

- How Television Works
- V-Chip Homepage - from the FCC

- Patent 4,554,584: Video and audio blanking system - A key V-chip patent
- Patent 5,828,402: Method and apparatus for selectively blocking audio and video signals
- V-chip information center
- FCC Docket
- What do movie ratings mean and who applies them?

Copyright © 1998-2003 Howstuffworks, Inc. All rights reserved.

Lycos (R) s a registered trademark of Carnegie Mellon University.

Privacy Policy | **Children's Privacy Notice** | Terms and Conditions | Standard Advertising Terms and Conditions

L Number	Hits	Search Text	DB	Time stamp
1	4	6047103.pn.,6314409.pn.,5724423.pn. and rule$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:11
2	6	6047103.pn.,6314409.pn.,5724423.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:12
3	3	6047103.pn.,6314409.pn.,5724423.pn. and rule$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:12
4	70	(STB or VTR or TV) and (enciph$ or decipher$ or encrypt$ or decrypt$) and different adj level	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:20
11	1650729	security near$5 level and different adj (encryption$ or encipher$)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:31
12	144	different adj security adj level	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:31
13	32768	(different adj security adj level) and different encryption$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:32
14	6	(different adj security adj level) and different adj encryption$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:32
15	0	((different adj security adj level) and different adj encryption$1) and @py<=1999	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:32
16	913	different adj (encryption$4 or encipher$4)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:35
17	295	(different adj (encryption$4 or encipher$4)) and @py<=1999	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:34
18	225	((different adj (encryption$4 or encipher$4)) and @py<=1999) and security	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:35
19	90	((different adj (encryption$4 or encipher$4)) and @py<=1999) and video	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:35
20	126	different adj (encryption$4 or encipher$4) with security	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:36

21	37	(different adj (encryption$4 or encipher$4) with security) and @py<=1999	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:36
-	95	AV and authenti$4 and key$	USPAT	2003/09/09 10:48
-	45	(AV and authenti$4 and key$) and rule$	USPAT	2003/09/08 16:55
-	31	((AV and authenti$4 and key$) and rule$) and @py<=2000	USPAT	2003/09/08 16:55
-	89	AV and authenti$4 and key$1	USPAT	2003/09/08 16:55
-	44	(AV and authenti$4 and key$1) and rule$	USPAT	2003/09/08 16:55
-	30	((AV and authenti$4 and key$1) and rule$) and @py<=2000	USPAT	2003/09/08 16:56
-	0	(((AV and authenti$4 and key$1) and rule$) and @py<=2000) and data with (important or signifi$5) with rule$1	USPAT	2003/09/08 16:57
-	23	(((AV and authenti$4 and key$1) and rule$) and @py<=2000) and data with (important or signifi$5) and rule$1	USPAT	2003/09/08 17:11
-	261	STB and TV	USPAT	2003/09/08 17:42
-	2	(STB and TV) and data adj significan$5	USPAT	2003/09/08 17:46
-	1	"5689559".PN.	USPAT	2003/09/08 17:45
-	1	"5761302".PN.	USPAT	2003/09/08 17:45
-	1	"4937679".PN.	USPAT	2003/09/08 17:46
-	2885	713/200,201,202,154,155,161,165,167-168,170.	USPAT	2003/09/08 17:47
-	4	713/200,201,202,154,155,161,165,167-168,170. and STB and TV	USPAT	2003/09/08 17:50
-	3	713/200,201,202,154,155,161,165,167-168,170. and STB and rule$1	USPAT	2003/09/08 17:52
-	376	705/57,67.ccls.	USPAT	2003/09/08 17:52
-	39013	705/57,67.ccls. and STB or TV	USPAT	2003/09/08 17:52
-	45	705/57,67.ccls. and (STB or TV)	USPAT	2003/09/08 17:53
-	9	(705/57,67.ccls. and (STB or TV)) and rule$1	USPAT	2003/09/08 18:03
-	585	711/163.ccls.	USPAT	2003/09/08 18:03
-	0	711/163.ccls. and data adj (rating or significan$5) with rule$	USPAT	2003/09/08 18:04
-	0	711/163.ccls. and data with rating with rule$	USPAT	2003/09/08 18:04
-	0	386/94.ccls. and rule$ and TSB and TV	USPAT	2003/09/08 18:05
-	9	386/94.ccls. and data with (rating or significan$6) and rule$1	USPAT	2003/09/08 18:11
-	156297	top adj set adj box$4 or TSB or TV	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:12
-	5197	(top adj set adj box$4 or TSB or TV) and (authentica$ or encrypt$5 or decrypt$5 or encipher$3 or decipher$3)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:13
-	1447	((top adj set adj box$4 or TSB or TV) and (authentica$ or encrypt$5 or decrypt$5 or encipher$3 or decipher$3)) and rule$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:13
-	103	(((top adj set adj box$4 or TSB or TV) and (authentica$ or encrypt$5 or decrypt$5 or encipher$3 or decipher$3)) and rule$1) and data with rating$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:14
-	3	(((top adj set adj box$4 or TSB or TV) and (authentica$ or encrypt$5 or decrypt$5 or encipher$3 or decipher$3)) and rule$1) and data with rating$1 with rule$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:17
-	0	380/5,20,201.ccls. and data with rating with rule$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:18

-	3	380/5,20,201.ccls. and data with rating	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:19
-	0	data adj rating with rule$ and TSB	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:20
-	0	data adj rating with rule$ and authentica$5	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:20
-	22	data with rating with rule$ and authentica$5	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/08 18:20
-	56	AV and authenti$4 and key$ and (encryp$5 or decrypt$5 or enciph$5 or deciph$)	USPAT	2003/09/09 12:10
-	42	((AV or audio) adj data) and transmit$5 and (different adj (level or rating$1 or rule$1)) and (encrypt$5 or decryp$5 or enciph$5 or deciph$5)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 11:02
-	152804	rule$ or (data adj rating) with (encrypt$4 or decrypt$4 and encipher$4 or decipher$4 or authenticat$4)	USPAT	2003/09/09 12:12
-	152804	(rule$ or (data adj rating) with (encrypt$4 or decrypt$4 and encipher$4 or decipher$4 or authenticat$4))	USPAT	2003/09/09 12:13
-	241868	(rule$ or (data adj rating)and(encrypt$4 or decrypt$4 and encipher$4 or decipher$4 or authenticat$4))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:13
-	241868	rule$ or (data adj rating) and (encrypt$4 or decrypt$4 and encipher$4 or decipher$4 or authenticat$4)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:14
-	0	(rule$ or (data adj rating) and (encrypt$4 or decrypt$4 and encipher$4 or decipher$4 or authenticat$4)) and TV and TSB and VTR	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:15
-	1	TV and TSB and VTR	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:23
-	1317	(rule or rating) and (enciph$5 or deciph$5 or encipher$5 or decipher$5)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:25
-	24	((rule or rating) and (enciph$5 or deciph$5 or encipher$5 or decipher$5)) and digital adj interface	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 12:32
-	84	different with level with encryption$1	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 17:30

-	7	(STB or VTR or TV) and (enciph$ or decipher$ or encrypt$ or decrypt$) and different adj level with security	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/09 13:44
-	0	"9941910"	USPAT; JPO	2003/09/10 12:38
-	0	9941910.pn.	USPAT; JPO	2003/09/10 12:38
-	0	WO99/41910	USPAT; JPO	2003/09/10 12:38
-	0	WO99/41910.pn.	USPAT; JPO	2003/09/10 12:39
-	0	WO99/41910.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 12:39
-	0	WO99/41910	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 12:42
-	0	WO9941910.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 12:43
-	0	WO/09941910.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 12:44
-	3	digital adj av adj data adj transmitting adj unit	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 13:08
-	8	digital and (av adj data) and (level with (rule$ or signific$5 or security)) and (encryp$5 or decrypt$5 or encipher$5 or decipher$5)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 15:08
-	2	5724423.pn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/09/10 15:18

L Number	Hits	Search Text	DB	Time stamp
1	801	common adj key	USPAT	2004/04/21 11:38
2	1	5987126.pn.	USPAT	2004/04/21 14:03
3	1522	((COMMON or public or private) adj key$1) and (rule$1 or policy)	USPAT	2004/04/21 14:07
5	112	(((COMMON or public or private) adj key$1) with (rule$1 or policy)) and (encrypt$5 or enciphe$5 or encod$5)	USPAT	2004/04/21 14:08
4	117	((COMMON or public or private) adj key$1) with (rule$1 or policy)	USPAT	2004/04/21 15:07
6	0	(common near5 key$1) near low near (security or (sensitive near data))	USPAT	2004/04/21 14:52
7	0	(common near5 key$1) near5 low near5 (security or (sensitive near data))	USPAT	2004/04/21 14:52
8	0	(common near5 key$1) near5 low with security	USPAT	2004/04/21 14:53
9	0	(common near5 key$1) near5 low near10 security	USPAT	2004/04/21 14:53
10	0	(common near10 key$1) near5 low near10 security	USPAT	2004/04/21 14:54
11	3	(common near10 key$1) near5 low near10 security	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:00
12	0	(common near10 key$1) near5 less near10 sensitive near10 data	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:01
13	0	(common near10 key$1) near5 less near10 sensitive	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:01
14	0	(common with key$1) near5 less near10 sensitive	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:01
15	0	(common with key$1) with less with sensitive .	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:01
16	0	(common with key$1) with less adj sensitive	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:02
17	4	(common with key$1) with (insignificant$4 or (less adj significant)) .	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/04/21 15:02
18	70	(((COMMON or public or private) adj key$1) with (rule$1 or policy)) and (sensitive or less$1sensitive or significant or less$1significant)	USPAT	2004/04/21 15:09
19	57	((((COMMON or public or private) adj key$1) with (rule$1 or policy)) and (sensitive or less$1sensitive or significant or less$1significant)) and (encrypt$ or enciph$6 or encod$6) with (common or asym$6 or public) with key$1	USPAT	2004/04/21 15:50
20	7	(common adj key$1) with (sensitive or significant)	USPAT	2004/04/21 15:55

21	0	(common adj key$1) with less near10 (sensitive or significant)	USPAT	2004/04/21 15:55
22	128	((public or asymetric$3) adj key$1) with (sensitive or significant)	USPAT	2004/04/21 15:56
23	42	(((public or asymetric$3) adj key$1) with (sensitive or significant)) and (common or symmetric$4) adj key$1	USPAT	2004/04/21 15:57
-	99	digital adj av	USPAT	2004/04/21 10:59

Conference Date: 2-5 Feb. 1981 Conference Location: Bahrain
Medium: Looseleaf
Language: English Document Type: Conference Paper (PA)
Treatment: New Developments (N); Practical (P)
Abstract: Communication are an extraordinarily important factor in most areas of modern life, but threatened in their reliability. This is true especially for military applications. Threats can be met by appropriate counter-measures. Among these countermeasures ciphering plays a dominant role. Ciphering and communications must be a working unity, but this necessity is limited by many constraints. To overcome the most stringent constraint, new requirements for a flexible cipher device are to be defined. On the basis of a modular design, AEG-Telefunken presents a **high - secure** , small-size, **low -cost cipher** system to meet the demands of modern communications. (0 Refs)
Subfile: B

17/7/7 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

03417434 E.I. Monthly No: EIM9204-020465
Title: High speed RSA processor.
Author: Al-Tuwaijry, F. A.; Barton, S. K.
Corporate Source: Univ of Bradford, Engl
Conference Title: 6th International Conference on Digital Processing of Signals in Communications
Conference Location: Loughborough, Engl Conference Date: 19910902
E.I. Conference No.: 16008
Source: IEE Conference Publication. Publ by IEE, Michael Faraday House, Stevenage, Engl. p 210-214
Publication Year: 1991
CODEN: IECPB4 ISSN: 0537-9987
Language: English
Document Type: PA; (Conference Paper) Treatment: T; (Theoretical); A; (Applications)
Journal Announcement: 9204
Abstract: With the explosion of electronic data communications and computer networks, it has become important to develop new ways to guarantee their security. Two techniques are available: the private key system (e.g. DES), and the public key systems (e.g. RSA). The private key systems are more widely used than the public key systems because they are fast and easy to implement, but they suffer from serious disadvantages such as **lower security** and complexity in distribution of the **key** . Public **key** systems provide much **higher security** levels and no need for **key** distribution. However, their use has been limited to **key** distribution for the private key systems because they are very slow. This paper describes three techniques for increasing the speed of the central computational process in the RSA algorithm, i.e. modular exponentiation. Together they achieve a speed improvement of about 7 to 1. (Author abstract) 7 Refs.

17/7/8 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci
(c) 2004 Inst for Sci Info. All rts. reserv.

09914787 Genuine Article#: BS63C Number of References: 12
Title: Privacy amplification secure against active adversaries
Author(s): Maurer U (REPRINT) ; Wolf S
Corporate Source: ETH Zurich,Swiss Fed Inst Technol, Dept Comp Sci,CH-8092

A HIGH SPEED RSA PROCESSOR

F A Al-Tuwaijry & S K Barton

University of Bradford. UK

ABSTRACT

With the explosion of electronic data communications and computer networks, it has become important to develop new ways to guarantee their security. Two techniques are available: the private key system (e.g. DES), and the public key systems (e.g. RSA).

The private key systems are more widely used than the public key systems because they are fast and easy to implement, but they suffer from serious disadvantages such as lower security and complexity in distribution of the key. Public key systems provide much higher security levels and no need for key distribution. However, their use has been limited to key distribution for the private key systems because they are very slow.

This paper describes three techniques for increasing the speed of the central computational process in the RSA algorithm, i.e. modular exponentiation. Together they achieve a speed improvement of about 7 to 1.

INTRODUCTION

This paper starts with a brief description of public key cryptosystems, and in particular the RSA algorithm, emphasising its high power but low speed. The modular exponentiation process is identified as the main source of time delay. Three techniques are discussed for increasing the speed of modular exponentiation.

Firstly, the order of examination of the bits of the exponent, Right-to-Left or Left-to-Right, can make a factor of two difference in execution time in the worst case. For a "typical" exponent, the improvement is 1.5 to 1.

Secondly, a bit pair re-coding technique based on the Booth algorithm gives a further 56% increase in speed.

Finally, a parallel implementation is discussed which achieves a further 3:1 increase in speed.

PUBLIC KEY CRYPTOSYSTEMS

The main feature which distinguishes public key from conventional cryptosystems such as DES [1] is the requirement for two keys rather than one. In conventional systems the same key is used for both encryption and decryption, and this leads to security problems in the distribution of keys. If an eavesdropper can discover the key during the process of passing it between transmitter and receiver, he can decipher the message.

The concept of public key cryptosystems was developed by Diffie and Hellman [2] and the first practical algorithm was publishsed by Rivest, Shamir and Adleman (RSA) [3]. The encryption process uses one of the two keys, and the decryption process the other. One key can therefore be published, provided that it is computationally infeasible for an eavesdropper to calculate the secret key from the public key.

A user wishing to send a message to user X encrypts it with X's public key, knowing that only X has the secret key required to decrypt the message. If X wants to send a "signed" message which could not have originated anywhere else, he encrypts it with his secret key. The recipient then decrypts it with X's public key.

RSA ALGORITHM

A user of the RSA cryptosystem creates his pair of keys as follows:

1. Two large prime numbers, p and q, are chosen at random (p and q are kept secret).
2. The modulus, $N=p.q$.
3. The Euler totient function, $\phi(N) = (p-1)(q-1)$. ($\phi(N)$ is kept secret).
4. A large integer, E, in the range $1<E<\phi(N)$, and coprime with $\phi(N)$ is chosen at random. E is the public encryption key.
5. The multiplicative inverse, D, of E modulo $\phi(N)$ is then determined from $D.E=1 \pmod{\phi(N)}$. D is the secret decryption key.
6. X announces the pair (E,N) as his public key, keeping the pair (D,N) as his secret key (p,q and $\phi(N)$ must also be kept secret).

Other users can then encrypt a message M using X's public key to produce ciphertext C, which can only be decrypted by X, as follows.

$$C = M^E \pmod{N}$$

X can decrypt the cipher text C using his secret key as follows

$$M' = C^D \pmod{N}$$

Proof that $M' = M$ is given in [3].

The security of the RSA cryptosystem depends on the difficulty for the cryptoanalyst of factoring the published modulus, N [4]. If the modulus can be factorised, the secret key (D,N) can be computed, enabling the cryptanalyst to read all private mail addressed to X, or forge his digital signature.

The best available algorithms for factoring large integers have a running time which is proportional to $\exp\{\ln(N).\ln(\ln(N))\}^{\frac{1}{2}}$ operations [4]. Assuming the computing time for one operation is one microsecond, and the wordlength K of N is 512 bits, the factorisation will take 9,755 years to complete. This is the basis on which the security of encryption algorithms is compared. The RSA algorithm offers a higher level of security than other cryptosystems, but at the expense of a slow operating speed, principally resulting from the modular exponentiation operation. It has therefore found application principally in secure key distribution for the faster conventional systems such as DES. The object of this presentation is to explore techniques for increasing the speed of the RSA implementation.

RSA IMPLEMENTATION

A block diagram of the RSA processor is shown in Fig. 1. There are four K-bit registers, which are used to hold the operands:

modulus	N
exponent	E or D
message	M or C
result	C or M'.

A 4-bit communication/status port and a 16-bit bi-directional data port are used to communicate with an external microprocessor controller. The internal controller maintains device status, controls the I/O ports and the Modular Exponentiation Logic. This circuitry performs the modular arithmetic, and is the critical element in determining the speed of the device.

MODULAR EXPONENTIATION

An efficient algorithm for computing M^E(mod N) is the approach of repeated squaring and multiplication [5]. There are two procedures having different properties, depending on the order of examination of the bits of the exponent [4]. The Left-to-Right (L-R) algorithm (Fig. 2a) deals with the most significant bit first, while the Right-to-Left (R-L) algorithm (Fig. 2b) deals with the least significant bit first.

Both algorithms execute K loops of the flowchart, where K is the number of bits in E represented as:

$$E = e_{K-1}2^{K-1} + e_{K-2}2^{K-2} + \ldots e_1 2 + e_0$$

One squaring operation is carried out in each loop. A further multiplication is performed only in those loops in which the exponent bit being examined, e_i, is set to ONE, and not when it is ZERO.

In the L-R algorithm the squaring operation must be completed before the multiplication, whereas in the R-L algorithm both operations can take place in parallel, see Figs. 3a and 3b. If the time taken to perform one multiplication is T, the time for a K-bit modular exponentiation is given by

$$T_{LR} = (K+E_1)T \qquad \text{(L-R)}$$

or

$$T_{RL} = KT \qquad \text{(R-L)}$$

where E_1 is the number of ONEs in E. The R-L algorithm is seen to be faster, but at the expense of needing to perform two multiplications in parallel, i.e. needing extra hardware.

If the choice of E is restricted to values with a small number of ONEs, the speed penalty of the L-R algorithm is small. However, a similar restriction applied to D would lead to a very limited choice of keys, and consequent reduced security. If no restrictions are placed on E_1, the L-R algorithm can take up to twice as long as the R-L. On average, E_1 will be equal to K/2, and the L-R algorithm will be 50% slower than R-L. A further disadvantage of L-R is that the processing speed is dependent on the choice of E. For the present application, where speed is more important that complexity, the R-L algorithm has been chosen.

MODULAR MULTIPLICATION

The time, T, taken for each operation is largely determined by the multipliers. Modular multiplication can be performed by integer multiplication of two K-bit numbers, followed by modulo reduction of the resulting 2K-bit number. The process of modulo reduction can be very time-consuming if performed at the end in this way. Multiplication can be executed significantly faster if modulo reduction is performed at each step of the multiplication process, so that the result never grows beyond K+1 bits. This technique, known as concurrent modular multiplication, also minimises storage space.

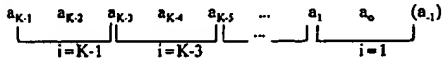
A flowchart for the conventional concurrent algorithm is given in Fig. 4. The K-bit multiplier, A, is represented as:

$$A = a_{K-1}2^{K-1} + a_{K-2}2^{K-2} \ldots a_1 2 + a_0$$

The multiplicand, B, and modulus, N, are also assumed to be K-bit words. K loops are required. In each loop the partial product P is multiplied by two and reduced modulo N, and the next bit is examined. If this is a ONE, then B is added to P and the result reduced modulo N. This means that modulo N reduction is always performed before P can possibly be greater than 2N, and hence involves only subtraction of N if P>N, or no operation if P<N. The time taken for a K-bit multiplication is $T_1 = Kt_1$, where t_1 is the loop time for the conventional algorithm. A minimum value of t_1 has been found to be 7t, where t is the clock cycle period. At a 10MHz clock rate, t_1 = 700ns.

A modified concurrent algorithm based on bit-pair re-coding, which is derived from the Booth technique, can give a significant reduction in processing time for only a marginal increase in complexity [6,7]. The flowchart of the modified concurrent algorithm is shown in Fig. 5.

The partial product is multiplied by four in each loop (multiplied by two and modulo reduced twice), and the bit pointer, i, moved two positions. The number of loops is therefore reduced to K/2, i.e. half that of the conventional algorithm, and the time required for a K-bit multiplication is $T_2 = t_2 K/2$, where t_2 is the loop time for the modified algorithm. In each loop three bits are examined: a_i, a_{i-1} and a_{i-2}. The last of these will be re-examined as a_i in the next loop when i is reduced by 2. Thus even-numbered bits are examined twice. An extra LSB, a_{-1}, assumed to be zero, is included for the final loop, as shown below:



The action in the rest of the loop is to add zero, ±B or ±2B to the partial product, depending on the state of the three bits, according to Table 1.

Table 1 Modified Concurrent Algorithm

a_i	a_{i-1}	a_{i-2}	Action
0	0	0	+0
0	0	1	+B
0	1	0	+B
0	1	1	+2B
1	0	0	-2B
1	0	1	-B
1	1	0	-B
1	1	1	+0

The values of -B (mod N) and ±2B (mod N) are pre-computed once for the entire calculation, so that only a single modulo reduction process is required at the end of the loop. The minimum number of clock cycles required to perform this loop has been calculated as $t_2 = 9t$, i.e. 900ns at 10MHz clock rate. For K = 512 bits, a standard implementation, the conventional and modified algorithms can be compared as follows:

$$T_1 = 512 \times 700 \text{ ns} = 358.4\mu s$$

$$T_2 = 512 \times 900/2 \text{ ns} = 230.4\mu s$$

The modified algorithm thus offers a 56% speed improvement at a cost of an increase in hardware complexity of about 10%.

PARALLEL IMPLEMENTATION

A further significant improvement in speed is achieved by the use of a parallel implementation, as shown in Figure 7. The K-bit multiplier is partitioned into J equal segments of K/J bits each, shown as A_{J-1} to A_0. These are each multiplied by B in a conventional or modified multiplier as described above. This takes:

$$T_J = \begin{cases} t_1 K/J \text{ (conventional)} \\ t_2 K/2J \text{ (modified)} \end{cases} \quad \text{clock cycles}$$

i.e. the time is reduced by a factor of J compared to the serial approach.

The required result is given by:

$$A.B = 2^{(J-1)K/J}A_{J-1}B + 2^{(J-2)K/J}A_{J-2}B + \ldots 2^{K/J}A_1B + A_0B$$

The outputs of the J multipliers are combined by a network of shift/subtract elements (SS) and add/subtract elements (AS). The SS elements shift the data K/J bits to the left, subtracting N from the total after each shift, as needed. The total delay through all the (J-1) rows of SS elements is $T_S = (J-1)K/J$ clock periods.

After each row, one of the segments has been shifted sufficiently and is added to the running total in an add/subtract element (AS). The delay through each of these is $T_A = 2t$, so this operation is completed before the next row of SS elements produces an output. Only the final AS element contributes to the total delay, which is

$$T_P = T_J + T_S + T_A$$

$$= \begin{cases} t_1 K/J + (J-1)t\ K/J + 2t & \text{(conventional)} \\ t_2 K/2J + (J-1)t\ K/J + 2t & \text{(modified)} \end{cases}$$

where t is the clock period.

Clearly $T_S + T_A$ is very nearly independent of J, and only T_J depends on J. T_P reduces rapidly with J at first, levelling off to an asymptote of (K+2)t for large J. A point of diminishing returns is reached when:

$$\begin{array}{lll} (J-1)t = t_1, & \text{i.e. } J = 8 & \text{(conventional)} \\ (J-1)t = t_2/2, & \text{i.e. } J = 5.5 & \text{(modified)} \end{array}$$

A value of J = 8, giving 64-bit segments, has been chosen for the present implementation, giving

$$T_P = \begin{cases} 7t \times 64 + 7t \times 64 + 2t = 898t \text{ (conventional)} \\ 9t \times 32 + 7t \times 64 + 2t = 738t \text{ (modified)} \end{cases}$$

The time required for a 512 bit modular exponentiation using the (R-L) algorithm is therefore

$$KT_p = \begin{cases} 459{,}776t = 46\text{ms} & \text{(conventional)} \\ 377{,}856t = 38\text{ms} & \text{(modified)} \end{cases}$$

The data rate which can be supported with a 10MHz clock rate is

$$K/KT_p = \begin{cases} 11.1 \text{ kb/s} & \text{(conventional)} \\ 13.5 \text{ kb/s} & \text{(modified)} \end{cases}$$

For comparison, a serial implementation of the conventional modular multiplication algorithm and (L-R) exponentiation would take:

$$T_{LR} = (K+E_1)T_1 = (K+E_1)Kt_1 = (512 + 256)512 \times 7t$$

$$= 2{,}752{,}512t = 275.25 \text{ ms}$$

The data rate supported with a 10MHz clock rate is therefore

$$K/(K+E_1)T_1 = 1.86 \text{ kb/s}$$

i.e. a factor of 7.28 slower.

CONCLUSIONS

This paper has discussed three techniques for increasing the speed of the modular exponentiation which is the core of the RSA public key cryptography algorithm. They are:

1. Right-to-Left exponentiation algorithm.
2. Modified (bit-pair) modular multiplication.
3. Parallel processing.

Taken together, the three techniques offer a speed improvement of about 7:1 over the conventional, Left-to-Right, serial approach.

REFERENCES

1. Data Encryption Standard (FIPS Pub), National Bureau of Standards, 15 January 1977.
2. W Diffie & M E Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, Vol. IT-22, No. 6, pp. 644-659, November 1976.
3. R L Rivest, A Shamir & L Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Com. of the ACM, Vol. 21, No.2, pp. 120-126, February 1978.
4. R L Rivest, "RSA Chips (Past/Present/Future)", Advances in Cryptology, Proc. of Eurocrypt 84, pp. 159-165, Springer-Verlag, Berlin, 1985.
5. D E Knuth, "The Art of Computer Programming", Vol. 2, Addison-Wesley, 2nd Edition, 1981.
6. K Hwang, "Computer Arithmetic: Principles, Architecture and Design", John Wiley & Sons, 1979.
7. J Cavanagh, "Digital Computer Arithmetic: Design and Implementation", McGraw Hill Book Company, 1985.

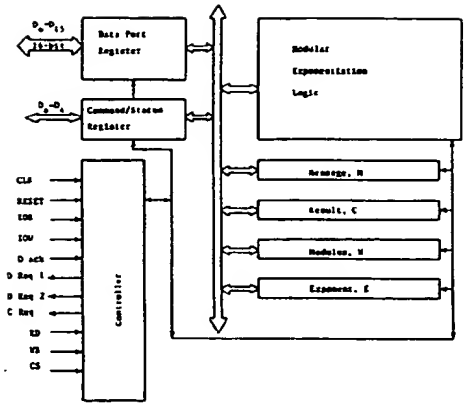


Figure 1 RSA Chip Block Diagram

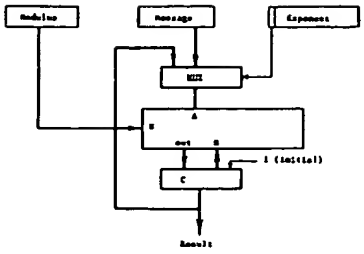


Figure 3a Block Diagram of Left-to-Right Algorithm

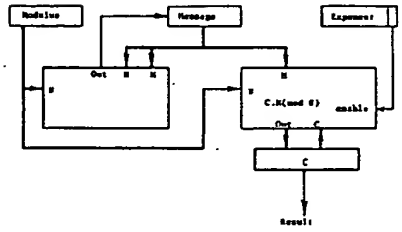


Figure 3b Block Diagram of Right-to-Left Algorithm

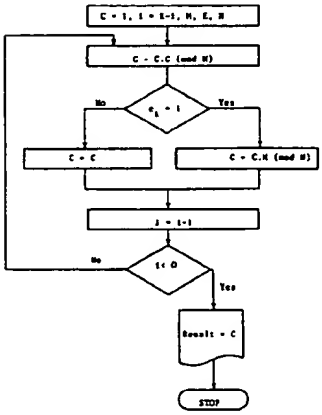


Figure 2a Left-to-Right Exponentiation Algorithm

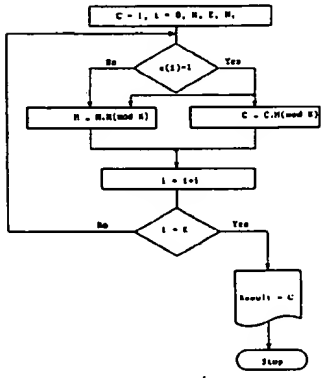


Figure 2b Right-to-Left Exponentiation Algorithm

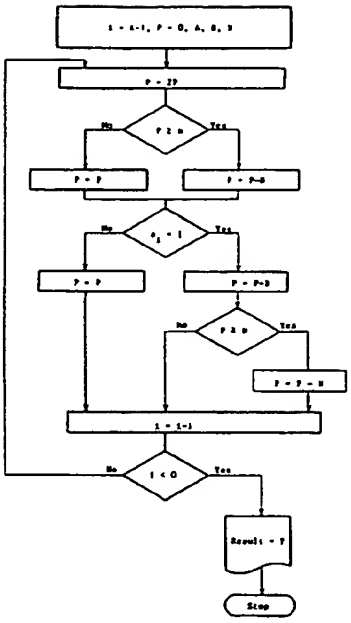


Figure 4 Conventional Concurrent Algorithm

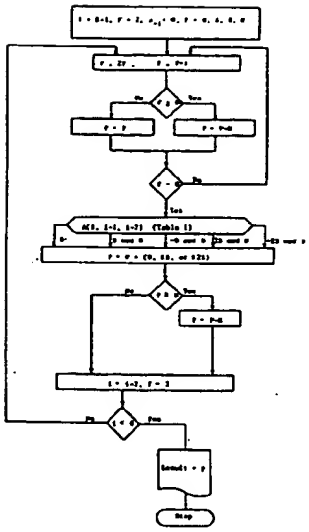


Figure 5 Modified Concurrent Algorithm

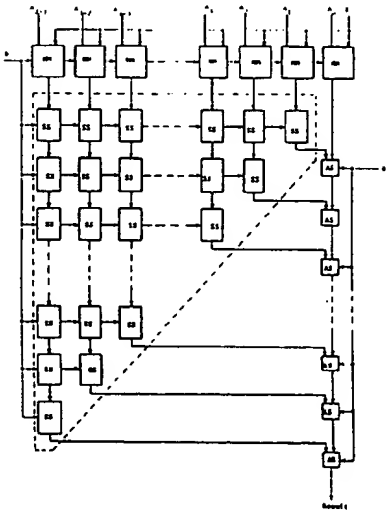


Figure 7 Block Diagram of Parallel Implementation

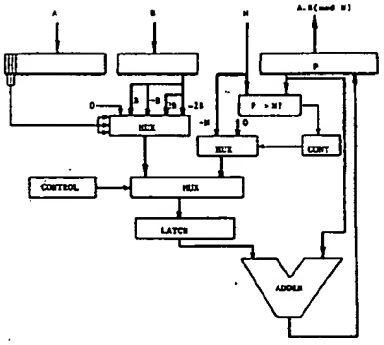


Figure 6 Block Diagram of Modified Concurrent Algorithm

File 348:EUROPEAN PATENTS 1978-2004/Apr W02
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	289089	KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM? OR KEY??????? ?
S2	1585	COMMON(1W)S1 OR COMMONKEY?
S3	12495	(PUBLIC OR ASYMMETRIC? OR SECRET OR SYMMETRIC OR CONVENTIONAL OR PRIVATE)(1W)S1 OR PRIVATEKEY? OR PUBLICKEY? OR SECRETKEY?
S4	402322	SECURITY OR SECURE? OR SECURING OR SECRET?
S5	16001	S4(2N)(HIGH??? ? OR MAXIMUM OR MAX OR GREAT??? ? OR MOST OR BEST OR OPTIMAL OR OPTIMAL OR OPTIMUM)
S6	367	S4(2N)(OPTIMIS? OR OPTIMIZ?)
S7	1	S4(2N)(MIN()MAX OR MINMAX)
S8	18294	S4(2N)(LOW??? ? OR MINIMUM OR MIN OR SLIGHT? OR LEAST)
S9	472	S2(25N)S3
S10	21	S9(25N)S5:S8
S11	21	IDPAT (sorted in duplicate/non-duplicate order)
S12	20	IDPAT (primary/non-duplicate records only)
S13	1385	S5:S6(15N)S1
S14	550	S7:S8(15N)S1
S15	63	S14(25N)S13
S16	6243	IC='H04L-009'
S17	20334	IC='H04N-007'
S18	11700	IC='H04N-001'
S19	13105	IC='G06F-001'
S20	27	S15 AND S16:S19
S21	25	S20 NOT S11
S22	25	IDPAT (sorted in duplicate/non-duplicate order)
S23	25	IDPAT (primary/non-duplicate records only)
S24	7	S15/TI,AB,CM
S25	3	S24 NOT (S23 OR S11)
S26	3	IDPAT (sorted in duplicate/non-duplicate order)
S27	3	IDPAT (primary/non-duplicate records only)
S28	33	S15 NOT (S11 OR S27 OR S23)
S29	33	IDPAT (sorted in duplicate/non-duplicate order)
S30	33	IDPAT (primary/non-duplicate records only)

12/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01371570

Optical disk, optical recorder, optical reproducer, cryptocommunication system and program license system

Optische Scheibe, optisches Aufzeichnungsgerat, optisches Wiedergabegerat, verschlusseltes Kommunikationssystem und Berechtigungssystem dafur

Enregistreur optique, dispositif optique de reproduction, systeme crypte de communications et systeme d'autorisations associe

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyogo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, Hikaridai 8-chome 6-4,Seikacho,, Souraku-gun,Kyoto 619-0237, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novapat International SA, 9, rue du Valais, 1202 Geneve, (CH)
PATENT (CC, No, Kind, Date): EP 1168328 A1 020102 (Basic)
APPLICATION (CC, No, Date): EP 2001120681 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 1024478 (EP 2000102970)
EP 802527 (EP 2096932845)
RELATED DIVISIONAL NUMBER(S) - PN (AN):
(EP 2003029684)

INTERNATIONAL PATENT CLASS: G11B-020/00; G06F-001/00; G11B-019/12

ABSTRACT EP 1168328 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020102 A1 Published application with search report
Examination: 020102 A1 Date of request for examination: 20010919
Change: 020424 A1 Inventor information changed: 20020307
Examination: 030507 A1 Date of dispatch of the first examination report: 20030320
Change: 040225 A1 Application number of divisional application (Article 76) changed: 20040109
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200201	93
SPEC A	(English)	200201	11662
Total word count - document A			11755
Total word count - document B			0
Total word count - documents A + B			11755

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01308279
A method and apparatus for designing cipher logic, and a computer product
Verfahren und Vorrichtung zum Entwurf einer Verschlusselungslogik und zugehoriger Computer
Procede et dispositif de conception d'une logique de chiffrage et ordinateur y relatif
PATENT ASSIGNEE:
FUJITSU LIMITED, (211463), 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP), (Proprietor designated states: all)
INVENTOR:
Shimoyama, Takeshi, Fujitsu Limited, 1-1, Kamikodanaka, 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa 211-8588, (JP)
LEGAL REPRESENTATIVE:
Stebbing, Timothy Charles et al (59641), Haseltine Lake & Co., Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)
PATENT (CC, No, Kind, Date): EP 1120933 A2 010801 (Basic)
EP 1120933 A3 020612
EP 1120933 B1 040324

APPLICATION (CC, No, Date): EP 2000311439 001220;
PRIORITY (CC, No, Date): JP 200016413 000126
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/06
CITED PATENTS (EP B): US 5778074 A; US 6031911 A
CITED REFERENCES (EP B):
PRENEEL B ET AL: "STATE OF THE ART IN APPLIED CRYPTOGRAPHY" COURSE ON COMPUTER SECURITY AND INDUSTRIAL CRYPTOGRAPHY. REVISED LECTURES, LEUVEN, BELGIUM, 3-6 JUNE 1997, pages 105-130, XP000979891 1997, Germany, Springer-Verlag, ISBN: 3-540-65474-7
SCHNEIER B ET AL: "Fast software encryption: designing encryption algorithms for optimal software speed on the Intel Pentium processor" FAST SOFTWARE ENCRYPTION. 4TH INTERNATIONAL WORKSHOP, FSE '97 PROCEEDINGS, FAST SOFTWARE ENCRYPTION. 4TH INTERNATIONAL WORKSHOP, FSE'97 PROCEEDINGS, HAIFA, ISRAEL, 20-22 JAN. 1997, pages 242-259, XP008002230 1997, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-63247-6;

ABSTRACT EP 1120933 A2
An optimization processing unit optimizes (S3) an input and output bit number of an S-box based on parameters inputted from an input unit. The examples of the parameters are memory capacity of a primary cache memory, entire input and output bit number, and smallest input and output number of the S-box. An S-box generating unit generates an S-box (54) in accordance with the optimized input and output bit number of the S-box. Then, an F-function generating unit generates an F-function (S5) by aligning a plurality of S-boxes thus generated.
ABSTRACT WORD COUNT: 90
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010801 A2 Published application without search report
Search Report: 020612 A3 Separate publication of the search report
Examination: 021002 A2 Date of request for examination: 20020729
Examination: 021204 A2 Date of dispatch of the first examination report: 20021017
Grant: 040324 B1 Granted patent
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200131	947
CLAIMS B	(English)	200413	1014
CLAIMS B	(German)	200413	878
CLAIMS B	(French)	200413	1259
SPEC A	(English)	200131	4920
SPEC B	(English)	200413	5097
Total word count - document A			5868
Total word count - document B			8248
Total word count - documents A + B			14116

...SPECIFICATION and satellite communications. However, it is necessary that such important information is transmitted in a **most secured** manner.

Various kinds of cipher protocols, such as secret-key cryptosystem or **public - key** cryptosystem, have been developed and used for transferring the information in a secured manner. The **secret - key** cryptosystem, which is a type of the **common key** block cipher, has proved to be most suitable for high-speed cipher communication.

A variety of cipher algorithms have been proposed as the **conventional**

common key block cipher. Most of such algorithms adopt a simple and repetitive structure referred to as...

...SPECIFICATION and satellite communications. However, it is necessary that such important information is transmitted in a **most secured** manner.

Various kinds of cipher protocols, such as secret-key cryptosystem or **public - key** cryptosystem, have been developed and used for transferring the information in a secured manner. The **secret - key** cryptosystem, which is a type of the **common key** block cipher, has proved to be most suitable for high-speed cipher communication.

A variety of cipher algorithms have been proposed as the **conventional common key** block cipher. Most of such algorithms adopt a simple and repetitive structure referred to as...

12/5,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01193349
METHOD OF CHECKING AUTHENTICITY OF SHEET WITH BUILT-IN ELECTRONIC CIRCUIT CHIP
VERFAHREN ZUR ECHTHEITSPRUFUNG EINES MIT EINGEBAUTEM SCHALTKREISCHIP VERSEHENEN BLATTES
PROCEDE PERMETTANT DE VERIFIER L'AUTHENTICITE D'UNE FEUILLE AU MOYEN D'UNE PUCE ELECTRONIQUE
PATENT ASSIGNEE:
Hitachi, Ltd., (204145), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
Hitachi Research Institute, (3047680), 6 Kanda Surugadai 4-chome, Chiyoda-ku, Tokyo 101-8010, (JP), (Applicant designated States: all)
INVENTOR:
OKAMOTO, Chikashi Sys. Dev. Lab., Hitachi Ltd., 1099, Ouzenji Asao-ku, Kawasaki-shi Kanagawa 215-0013, (JP)
TAKARAGI, Kazuo Sys. Dev. Lab., Hitachi Ltd., 1099, Ouzenji Asao-ku, Kawasaki-shi Kanagawa 215-0013, (JP)
TSUJI, Kazutaka Ctr. Res. Lab., Hitachi Ltd., 280, Higashikoigakubo 1-chome, Kokubunji-shi Tokyo 185-8601, (JP)
USAMI, Mitsuo Ctr. Res. Lab., Hitachi Ltd., 280, Higashikoigakubo 1-chome , Kokubunji-shi Tokyo 185-8601, (JP)
YASUNOBU, Chizuko Hitachi Research Institute, 6, Kanda Surugadai 4-chome Chiyoda-ku, Tokyo 101-8010, (JP)
ISOBE, Asahiko Hitachi Research Institute, 6, Kanda Surugadai 4-chome Chiyoda-ku, Tokyo 101-8010, (JP)
TSUNEMI, Yasuhiro Hitachi Research Institute, 6, Kanda Surugadai 4-chome Chiyoda-ku, Tokyo 101-8010, (JP)
YAGI, Hiroyuki Hitachi Research Institute, 6, Kandasurugadai 4-chome Chiyoda-ku, Tokyo 101-8010, (JP)
LEGAL REPRESENTATIVE:
Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1139302 A1 011004 (Basic)
WO 200034923 000615
APPLICATION (CC, No, Date): EP 99973338 991203; WO 99JP6798 991203
PRIORITY (CC, No, Date): JP 98346738 981207
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G07D-007/06; G06K-019/073; B42D-015/10

CITED PATENTS (WO A): JP 57161993 A ; JP 10291391 A ; JP 7085172 A ; JP 4248695 A ; US 5601931 A ; JP 3188590 A

ABSTRACT EP 1139302 A1

A method of checking sheets as to forgery thereof, the sheet being provided with an electronic circuit chip from or in which information can be read out or written and having visible information. The method includes

a step of encrypting the visible information of the sheet and storing the encrypted visible information in the electronic circuit chip, and a step of determining discriminatively the authenticity of the sheet by comparing the visible information of the sheet with the information stored in the electronic circuit chip.

ABSTRACT WORD COUNT: 87

NOTE:
Figure number on first page: 10

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000920	A1	International application. (Art. 158(1))
Application:	000920	A1	International application entering European phase
Application:	011004	A1	Published application with search report
Examination:	011004	A1	Date of request for examination: 20010703

LANGUAGE (Publication,Procedural,Application): English; English; Japanese

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200140	492
SPEC A	(English)	200140	8061
Total word count - document A			8553
Total word count - document B			0
Total word count - documents A + B			8553

...SPECIFICATION the electronic circuit chip is important or the volume of the information is large, the **public key** cryptosystem should preferably be adopted while the **common key** cryptosystem may advantageously be employed in the case where the authenticity of the sheet must be checked at a high speed. When the **public key** cryptosystem is adopted, the memory as required may be of a small capacity because the length of the key is short with **high security** being ensured because of impossibility of estimating the encrypting key from the key for decryption...

12/5,K/6 (Item 6 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

01174493

Optical disk for use with an encryption or program license system

Optische Platte zur Anwendung in einem Verschlussel- oder Programmlizenzsystem

Disque optique utilise dans un systeme crypte ou un systeme d'autorisations

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)

INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)

Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)

LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)

PATENT (CC, No, Kind, Date): EP 1024478 A1 000802 (Basic)
EP 1024478 B1 020502

APPLICATION (CC, No, Date): EP 2000102970 961008;

PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809

DESIGNATED STATES: DE; FR; GB

RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)

RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1168328 (EP 2001120681)

INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12

CITED PATENTS (EP B): EP 549488 A; EP 741382 A; US 4677604 A

CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1024478 A1

The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.

ABSTRACT WORD COUNT: 82

NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000802	A1	Published application with search report
Examination:	000802	A1	Date of request for examination: 20000301
Change:	001115	A1	Inventor information changed: 20000925
Examination:	001129	A1	Date of dispatch of the first examination report: 20001011
Change:	011024	A1	Title of invention (German) changed: 20010906
Change:	011024	A1	Application number of divisional application (Article 76) changed: 20010906
Grant:	020502	B1	Granted patent
Oppn None:	030423	B1	No opposition filed: 20030204

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200031	73
CLAIMS B	(English)	200218	101
CLAIMS B	(German)	200218	99
CLAIMS B	(French)	200218	119
SPEC A	(English)	200031	11662
SPEC B	(English)	200218	11797
Total word count - document A			11736
Total word count - document B			12116

Total word count - documents A + B 23852

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152851
Optical recorder and optical recording method using encryption
Optisches Aufzeichnungsgerat und Aufzeichnungsverfahren mit Verschlusselung
Enregistreur optique et procede d'enregistration crypte
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)
PATENT (CC, No, Kind, Date): EP 1005028 A1 000531 (Basic)
EP 1005028 B1 020424
APPLICATION (CC, No, Date): EP 2000102971 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 549488 A; EP 565281 A; EP 741382 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005028 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft

ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 000531 A1 Published application with search report
Examination: 000531 A1 Date of request for examination: 20000301
Change: 001115 A1 Inventor information changed: 20000925
Examination: 001129 A1 Date of dispatch of the first examination report: 20001013
Change: 011004 A1 Title of invention (German) changed: 20010810
Change: 011004 A1 Title of invention (English) changed: 20010810
Change: 011004 A1 Title of invention (French) changed: 20010810
Grant: 020424 B1 Granted patent
Oppn None: 030416 B1 No opposition filed: 20030127
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	2474
CLAIMS B	(English)	200217	394
CLAIMS B	(German)	200217	336
CLAIMS B	(French)	200217	465
SPEC A	(English)	200022	11662
SPEC B	(English)	200217	11951
Total word count - document A			14138
Total word count - document B			13146
Total word count - documents A + B			27284

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common** key , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152850
Optical recorder
Optisches Aufzeichnungsgerat
Enregistreur optique
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto

610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novapat International SA, 9, rue du Valais, 1202 Geneve, (CH)
PATENT (CC, No, Kind, Date): EP 1005027 A1 000531 (Basic)
EP 1005027 B1 010523
APPLICATION (CC, No, Date): EP 2000102969 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 565281 A; EP 741382 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005027 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000531	A1	Published application with search report
Examination:	000531	A1	Date of request for examination: 20000301
Change:	001115	A1	Inventor information changed: 20000925
Change:	001129	A1	Title of invention (German) changed: 20001009
Change:	001129	A1	Title of invention (English) changed: 20001009
Change:	001129	A1	Title of invention (French) changed: 20001009
Examination:	010110	A1	Date of dispatch of the first examination report: 20001130
Change:	010523	A1	Title of invention (German) changed: 20010404
Grant:	010523	B1	Granted patent
Oppn None:	020522	B1	No opposition filed: 20020226

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	283
CLAIMS B	(English)	200121	284
CLAIMS B	(German)	200121	258
CLAIMS B	(French)	200121	348
SPEC A	(English)	200022	11661
SPEC B	(English)	200121	11674
Total word count - document A			11945
Total word count - document B			12564
Total word count - documents A + B			24509

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/9 (Item 9 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152849

Optical recorder
Optisches Aufzeichnungsgerat
Enregistreur optique

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novapat International SA, 9, rue du Valais, 1202 Geneve, (CH)

PATENT (CC, No, Kind, Date): EP 1005026 A1 000531 (Basic)
EP 1005026 B1 010523
APPLICATION (CC, No, Date): EP 2000102968 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 565281 A; EP 741382 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005026 A1

The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures

are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000531	A1	Published application with search report
Examination:	000531	A1	Date of request for examination: 20000301
Change:	001115	A1	Inventor information changed: 20000925
Change:	001129	A1	Title of invention (German) changed: 20001009
Change:	001129	A1	Title of invention (English) changed: 20001009
Change:	001129	A1	Title of invention (French) changed: 20001009
Examination:	010110	A1	Date of dispatch of the first examination report: 20001130
Grant:	010523	B1	Granted patent
Oppn None:	020522	B1	No opposition filed: 20020226

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	274
CLAIMS B	(English)	200121	275
CLAIMS B	(German)	200121	243
CLAIMS B	(French)	200121	337
SPEC A	(English)	200022	11661
SPEC B	(English)	200121	11672
Total word count - document A			11936
Total word count - document B			12527
Total word count - documents A + B			24463

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152848
Optical disk for use with an encryption or program license system
Optische Platte zur Anwendung in einem Verschlussel- oder Programmlizenzsystem
Disque optique pour utilisation avec un systeme d'encryptage ou d'autorisation d'utilisation des logiciels
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)

Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)

LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novapat International SA, 9, rue du Valais, 1202 Geneve, (CH)

PATENT (CC, No, Kind, Date): EP 1005025 A1 000531 (Basic)
EP 1005025 B1 020102

APPLICATION (CC, No, Date): EP 2000102967 961008;

PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809

DESIGNATED STATES: DE; FR; GB

RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)

INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12

CITED PATENTS (EP B): EP 549488 A; EP 741382 A; US 4677604 A

CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005025 A1

The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.

ABSTRACT WORD COUNT: 82

NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000531	A1	Published application with search report
Examination:	000531	A1	Date of request for examination: 20000301
Change:	001115	A1	Inventor information changed: 20000925
Change:	001129	A1	Title of invention (German) changed: 20001009
Change:	010103	A1	Title of invention (German) changed: 20001114
Change:	010103	A1	Title of invention (French) changed: 20001114
Examination:	010207	A1	Date of dispatch of the first examination report: 20001227
Grant:	020102	B1	Granted patent
Oppn None:	030102	B1	No opposition filed: 20021003

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	91
CLAIMS B	(English)	200201	123
CLAIMS B	(German)	200201	114
CLAIMS B	(French)	200201	142
SPEC A	(English)	200022	11661
SPEC B	(English)	200201	11672
Total word count - document A			11753
Total word count - document B			12051
Total word count - documents A + B			23804

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152847
Optical reproducing device for the reproduction of encrypted information
Optisches Wiedergabegerat zur Wiedergabe verschlusselter Informationen
Appareil de reproduction optique pour la reproduction de l'information cryptee
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashiakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)
Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novapat International SA, 9, rue du Valais, 1202 Geneve, (CH)
PATENT (CC, No, Kind, Date): EP 1005024 A1 000531 (Basic)
EP 1005024 B1 010530
APPLICATION (CC, No, Date): EP 2000102966 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 565281 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005024 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft

ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 000531 A1 Published application with search report
Examination: 000531 A1 Date of request for examination: 20000301
Change: 000927 A1 Inventor information changed: 20000810
Examination: 010110 A1 Date of dispatch of the first examination report: 20001130
Grant: 010530 B1 Granted patent
Oppn None: 020522 B1 No opposition filed: 20020301
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	301
CLAIMS B	(English)	200122	303
CLAIMS B	(German)	200122	290
CLAIMS B	(French)	200122	389
SPEC A	(English)	200022	11663
SPEC B	(English)	200122	11669
Total word count - document A			11965
Total word count - document B			12651
Total word count - documents A + B			24616

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/12 (Item 12 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01152846
Optical reproducing device for the reproduction of encrypted information
Optisches Wiedergabegerat zur Wiedergabe verschlusselter Informationen
Appareil de reproduction pour la reproduction de l'information cryptee
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Katsura-minamitatsumi-cho, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, 5-1-3, Higashinakahama, Joto-ku,, Osaka-shi, Osaka 536-0023, (JP)
Tanaka, Shinichi, 1-42-14, Yamate-higashi, Tanabe-cho, Tuzuki-gun, Kyoto 610-03, (JP)
Koishi, Kenji, 3-56-8, Keyakidai, Sanda-shi, Hyougo 669-13, (JP)
Moriya, Mitsurou, 1-29, Hikarigaoka 3-chome, Ikoma-shi, Nara 630-01, (JP)

Takemura, Yoshinari, 2-8-11, Befu, Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Balsters, Robert et al (83702), Novagraaf SA 25, Avenue du Pailly, 1220 Les Avanchets - Geneva, (CH)
PATENT (CC, No, Kind, Date): EP 1005023 A1 000531 (Basic)
EP 1005023 B1 020522
APPLICATION (CC, No, Date): EP 2000102965 961008;
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 802527 (EP 96932845)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 565281 A; EP 741382 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 (1992-10-14) & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992 (1992-06-25);

ABSTRACT EP 1005023 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: NONE

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	000531	A1	Published application with search report
Examination:	000531	A1	Date of request for examination: 20000301
Change:	001115	A1	Inventor information changed: 20000925
Examination:	010110	A1	Date of dispatch of the first examination report: 20001130
Grant:	020522	B1	Granted patent
Oppn None:	030514	B1	No opposition filed: 20030225

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200022	254
CLAIMS B	(English)	200221	255
CLAIMS B	(German)	200221	241
CLAIMS B	(French)	200221	320
SPEC A	(English)	200022	11663
SPEC B	(English)	200221	11718
Total word count - document A			11918
Total word count - document B			12534
Total word count - documents A + B			24452

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding

key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

12/5,K/13 (Item 13 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00975147
Digital copyright management system using electronic watermark
Urheberrechtsdatenverwaltungssystem mit elektronischem Wasserzeichen
Systeme de gestion de donnees de droits d'auteurs avec une filigraine electronique
PATENT ASSIGNEE:
MITSUBISHI CORPORATION, (653510), 6-3, Marunouchi 2-chome, Chiyoda-ku Tokyo 100, (JP), (applicant designated states: AT;BE;CH;CY;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Saito, Makoto, 2-12-6-104, Kaitori, Tama-shi, (JP)
LEGAL REPRESENTATIVE:
Gleiter, Hermann et al (91481), Pfenning, Meinig & Partner GbR Mozartstrasse 17, 80336 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 884669 A2 981216 (Basic)
EP 884669 A3 990506
APPLICATION (CC, No, Date): EP 98110563 980609;
PRIORITY (CC, No, Date): JP 97173168 970613
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G06F-001/00; G06F-009/46; H04N-001/32; H04L-009/08;

ABSTRACT EP 884669 A2
A system for managing a digital content, particularly a digital content to which a copyright is claimed, and a system for supplying a public-key which is used in the management of the digital content are provided. The digital content management program is embedded to an operating system of a user apparatus as a micro-kernel, a watch program or a watch command which is linked to the digital content management program is transmitted to the user apparatus by using a network or data broadcasting, and thereby, the illegitimate usage of the digital content is watched. A visible watermark is added to the digital content when illegitimately utilized, to restrain later usage. Even in regular usage, the route of copying or transferring the digital content can also be ascertained by adding an invisible watermark. Further, a public-key is put in a public-key distribution screen to be distributed by the network or broadcasting. Image data to which information on owner of the public-key or on the user is added as an invisible electronic watermark, is entered to the public-key distribution screen, so that the authenticity of the public-key and the user is checked by the electronic watermark.
ABSTRACT WORD COUNT: 195

LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	010523 A2	Date of dispatch of the first examination report: 20010403
Application:	981216 A2	Published application (A1with Search Report ;A2without Search Report)
Change:	020918 A2	Legal representative(s) changed 20020729
Change:	990414 A2	Obligatory supplementary classification (change)
Search Report:	990506 A3	Separate publication of the European or

International search report
Examination: 991229 A2 Date of request for examination: 19991029
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9851	639
SPEC A	(English)	9851	8250
Total word count - document A			8889
Total word count - document B			0
Total word count - documents A + B			8889

...SPECIFICATION center which transmits the watch program via a network.
Next, an embodiment for distributing a **public - key** is described.
The size of a crypt key used in the **secret - key** cryptosystem, which is also referred to as a **common key** system, is about 100 bits at the largest, whereas the size of the crypt key which is used in the **public - key** cryptosystem exceeds 1000 bits in the case of a large one. The public-key cryptosystem has **high security** , and on the other hand, performing the encryption and decryption is rather complex, and therefore ...

12/5,K/14 (Item 14 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00854146
RECORDER FOR OPTICAL DISKS
AUFZEICHNUNGSGERAT FUR OPTISCHE PLATTEN
ENREGISTREUR POUR DISQUES OPTIQUES
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
OSHIMA, Mitsuaki, 115-3, Minamitatsumi-cho Katsura Nishikyo-ku, Kyoto-shi Kyoto 615, (JP)
GOTOH, Yoshiho, 4-9-17-201, Higashi-Nakahama Jyouto-ku Osaka-shi, Osaka 536, (JP)
TANAKA, Shinichi, 1-42-14, Yamate-higashi Tanabe-cho Tuzuki-gun, Kyoto 610-03, (JP)
KOISHI, Kenji, 3-56-8, Keyakidai, Sanda-shi Hyougo 669-13, (JP)
MORIYA, Mitsurou, 1-29, Hikarigoaka 3-chome Ikoma-shi, Nara 630-01, (JP)
TAKEMURA, Yoshinari, 2-8-11, Befu Settu-shi, Osaka 566, (JP)
LEGAL REPRESENTATIVE:
Kugele, Bernhard et al (51541), NOVAPAT INTERNATIONAL SA, 9, Rue du Valais, 1202 Geneve, (CH)
PATENT (CC, No, Kind, Date): EP 802527 A1 971022 (Basic)
EP 802527 A1 971210
EP 802527 B1 010829
WO 9714144 970417
APPLICATION (CC, No, Date): EP 96932845 961008; WO 96JP2924 961008
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123; JP 96211304 960809
DESIGNATED STATES: DE; FR; GB
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1005023 (EP 2000102965)
EP 1005024 (EP 2000102966)
EP 1005025 (EP 2000102967)
EP 1005026 (EP 2000102968)
EP 1005027 (EP 2000102969)

EP 1024478 (EP 2000102970)
EP 1005028 (EP 2000102971)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G06F-012/14; G06F-009/06; G11B-020/00; G06F-001/00; G11B-019/12
CITED PATENTS (EP B): EP 549488 A; EP 565281 A; EP 741382 A; EP 807929 A; JP 2293930 A; JP 58021143 A; JP 61071487 A; US 4677604 A
CITED REFERENCES (EP B):
PATENT ABSTRACTS OF JAPAN vol. 016, no. 495 (P-1436), 14 October 1992 & JP 04 178967 A (DAINIPPON PRINTING CO LTD), 25 June 1992,
SHINGAKU GIHO, Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, 21 September 1994, MAKOTO YOSHIOKA, RYOTA AKIYAMA, "Trend of Superdistribution Technology", pages 67-74.
SHINGAKU GIHO, Vol. 94, No. 240, Technical Paper of the Inst. of Electronics, Information and Communication Engineers of Japan, Information Security, ISEC94-13-22, 21 September 1994, YOSHIMICHI NAKAZAWA, "Software Distribution Technology with CD-ROM", pages 41-46.;

ABSTRACT EP 802527 A1
The operating and other procedures of an optical disk application system of the type for which a network is used are simplified. Optical disks have auxiliary data recording areas, where different IDs for individual disks, and/or cipher keys and/or decoding keys for ciphers are recorded in advance in a factory. By using the IDs to release the soft ciphers, using the cipher keys when sending the ciphers, and using the decoding keys when receiving the ciphers, user authorization procedures are simplified.
ABSTRACT WORD COUNT: 82
NOTE:
Figure number on first page: 1
LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	000614	A1 Date of dispatch of the first examination report: 20000427
Change:	20000405	A1 Application number of divisional application (Article 76) changed: 20000216
Oppn None:	020821	B1 No opposition filed: 20020530
Change:	010328	A1 Title of invention (French) changed: 20010202
Change:	010328	A1 Title of invention (English) changed: 20010202
Change:	010328	A1 Title of invention (German) changed: 20010202
Change:	010321	A1 Title of invention (German) changed: 20010201
Change:	010321	A1 Title of invention (English) changed: 20010201
Change:	010321	A1 Title of invention (French) changed: 20010201
Grant:	010829	B1 Granted patent
Application:	970806	A1 International application (Art. 158(1))
Application:	971022	A1 Published application (A1with Search Report ;A2without Search Report)
Examination:	971022	A1 Date of filing of request for examination: 970707
Change:	971203	A1 Obligatory supplementary classification (change)
Search Report:	971210	A1 Drawing up of a supplementary European search report: 971022

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199710W3	2477
CLAIMS B	(English)	200135	273
CLAIMS B	(German)	200135	239
CLAIMS B	(French)	200135	324
SPEC A	(English)	199710W3	11663
SPEC B	(English)	200135	11696

Total word count - document A 14142
Total word count - document B 12532
Total word count - documents A + B 26674

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...

...SPECIFICATION 838a has generated a pair of a cipher key and a decoding key of a **public key cipher** , not a **common key** , it is possible to make the **security higher** than that with the **common key** , though the processing time is longer, by cryptically sending the cipher key to the second...
? t12/5,k/19-20

12/5,K/19 (Item 19 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00557714 **Image available**
DEVICE AND METHOD FOR RECORDING, REPRODUCING AND PROCESSING DATA
DISPOSITIF ET PROCEDE D'ENREGISTREMENT, DE REPRODUCTION ET DE TRAITEMENT DE DONNEES
Patent Applicant/Assignee:
MATSUSHITA ELECTRIC INDUSTRIAL CO LTD,
Inventor(s):
TAGAWA Kenji,
MINAMI Masataka,
KOZUKA Masayuki,
AOYAMA Shoichi,
TOKUDA Katsumi,
HIRATA Noboru,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200021087 A2 20000413 (WO 0021087)
Application: WO 99JP5516 19991007 (PCT/WO JP9905516)
Priority Application: JP 98286177 19981008; JP 98297159 19981019; JP 98297142 19981019
Designated States: AU CN ID KR MX VN DE FR GB NL
Main International Patent Class: G11B-020/00
International Patent Class: H04N-007/167; H04N-007/26; H04N-005/913; G06F-001/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 19103

English Abstract
A recording medium stores a retail content and a superdistribution content that is encrypted according to a block cryptosystem. A superdistribution header is attached to the superdistribution content and encrypted according to a public key cryptosystem. The superdistribution header contains a decryption key used to decrypt the block cryptosystem. The public key cryptosystem is characterized by using a device connected to a communication network for decryption. The decryption is performed when the recording medium is loaded into the device with a fee being charged via the communication network.

French Abstract

File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200426
(c) 2004 Thomson Derwent

Set	Items	Description
S1	321082	KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM? OR KEY??????? ?
S2	1213	COMMON(1W)S1 OR COMMONKEY?
S3	5967	(PUBLIC OR ASYMMETRIC? OR SECRET OR SYMMETRIC OR CONVENTIONAL OR PRIVATE)(1W)S1 OR PRIVATEKEY? OR PUBLICKEY? OR SECRETKEY?
S4	708883	SECURITY OR SECURE? OR SECURING OR SECRET?
S5	15972	S4(2N)(HIGH??? ? OR MAXIMUM OR MAX OR GREAT??? ? OR MOST OR BEST OR OPTIMAL OR OPTIMAL OR OPTIMUM)
S6	79	S4(2N)(OPTIMIS? OR OPTIMIZ?)
S7	0	S4(2N)(MIN()MAX OR MINMAX)
S8	11348	S4(2N)(LOW??? ? OR MINIMUM OR MIN OR SLIGHT? OR LEAST)
S9	320	S2 AND S3
S10	19	S9 AND S5:S8
S11	43	S1 AND S5:S6 AND S8
S12	43	S11 NOT S10
S13	43	IDPAT (sorted in duplicate/non-duplicate order)
S14	42	IDPAT (primary/non-duplicate records only)

10/9/15 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013105820 **Image available**
WPI Acc No: 2000-277691/200024
XRPX Acc No: N00-209034

Key management method for encryption communication system, involves generating session key and disclosure key using common **key and time information**

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2000075788	A	20000314	JP 98247452	A	1998090	200024	B

Priority Applications (No Type Date): JP 98247452 A 19980901
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000075788	A		14	G09C-001/00	

Abstract (Basic): JP 2000075788 A

NOVELTY - Session and disclosure keys are generated using **common key** and time information. The time information is encrypted by session key and is considered as execution consent information. The session key belongs to key storage group which is in **lower** order from **secret key** of transmission side user apparatus, while the disclosure key belongs to higher order group from that of the receiver side user apparatus.

DETAILED DESCRIPTION - When the next session key is generated and there is no group in lower order from the execution consent information, the **secret key** of the transmission side user apparatus, the **common key** which consists of disclosure key of receiving side user apparatus and the time information are transmitted to the receiving side user apparatus and the message is encrypted using the session key. Appending information which includes time information is generated and is transmitted to the receiving side user apparatus.

INDEPENDENT CLAIMS are also included for the following:

(a) key management method;
(b) key management apparatus;
(c) program for key management

USE - For encryption communication system.

ADVANTAGE - The number of system T required for decoding in each hierarchy can be set-up independently. Comparison of appending information is not needed at the receiving side.

pp; 14 DwgNo 1/13

Title Terms: KEY; MANAGEMENT; METHOD; ENCRYPTION; COMMUNICATE; SYSTEM; GENERATE; SESSION; KEY; DISCLOSE; KEY; COMMON; KEY; TIME; INFORMATION
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00
International Patent Class (Additional): H04L-009/08
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): W01-A05A

? t14/9/2,6,13

14/9/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

015575988 **Image available**
WPI Acc No: 2003-638145/200361
XRPX Acc No: N03-507696
Relational database system for encryption of individual data elements, in which each data element which is to be protected is assigned an attribute indicating level of encryption needed
Patent Assignee: PROTEGRITY RES & DEV (PROT-N)
Inventor: MATTSSON U
Number of Countries: 026 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1207443	A2	20020522	EP 2001126668	A	20011108	200361	B
SE 200004189	A	20020517	SE 20004189	A	20001116	200361	
SE 517808	C2	20020716	SE 20004189	A	20001116	200361	

Priority Applications (No Type Date): SE 20004189 A 20001116
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1207443	A2	E	7	G06F-001/00	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR				
SE 200004189	A			G06F-001/00	
SE 517808	C2			G06F-001/00	

Abstract (Basic): EP 1207443 A2
NOVELTY - Several different encryption processes are carried out utilizing categories master **keys** like data encryption **keys** , **key** encryption **keys** held in encryption devices. The **higher security** level process utilizes a tamper- proof hardware device to a higher degree compared to **lower security** level process. Each data element which is to be protected is assigned an attribute indicating the level of encryption needed.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a method of encryption of individual data elements.
USE - For encryption of individual data elements.
ADVANTAGE - Improves flexibility and overall performance in encryption data while reducing load on tamper-proof hardware device.
DESCRIPTION OF DRAWING(S) - The figure shows the schematic view of the relational database system.
pp; 7 DwgNo 1/1
Title Terms: RELATED; DATABASE; SYSTEM; ENCRYPTION; INDIVIDUAL; DATA; ELEMENT; DATA; ELEMENT; PROTECT; ASSIGN; ATTRIBUTE; INDICATE; LEVEL; ENCRYPTION; NEED
Derwent Class: T01
International Patent Class (Main): G06F-001/00
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-J05B4B

14/9/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014715909 **Image available**

WPI Acc No: 2002-536613/200257
XRPX Acc No: N02-424940

Data administration method for electronic data stored in magnetic disk, floppy disk, DVD, involves embedding consent information containing information on encryption key in header data section as electronic watermark

Patent Assignee: FUJITSU LTD (FUIT); HASHIMOTO S (HASH-I); HATTORI E (HATT-I); HIRANO H (HIRA-I); MOCHIZUKI S (MOCH-I)
Inventor: HASHIMOTO S; HATTORI E; HIRANO H; MOCHIZUKI S
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20020059522	A1	20020516	US 2001811550	A	20010320	200257	B
JP 2002152490	A	20020524	JP 2000342753	A	20001110	200257	

Priority Applications (No Type Date): JP 2000342753 A 20001110
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020059522	A1		26	H04L-009/32	
JP 2002152490	A		15	H04N-001/387	

Abstract (Basic): US 20020059522 A1

NOVELTY - A header data section (16) is prepared for visual or auditory recognition of digital content attributes. A consent information (13) added to section (16) containing consent data on an encryption **key** in encrypting digital content is embedded in section (16) as an electronic watermark. A composite data is prepared in which a real data section (15) and consent data added header data section are composited, thereby distributing composite data.

USE - For data administration in computer program and in electronic publication and for electronic data stored on magneto optical disk, digital video disk, floppy disk, mini disk, etc.

ADVANTAGE - The digital content **high** in **security** request is encrypted by using the encryption **key** to maintain the security effect and the digital content **low** in the **security** request omits the encrypting, whereby a reduction in period of time for producing the synthetic data at that time of distribution and reduction in period of time for starting at the time of using can be made.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram explaining the data administration method.

Consent information (13)
Real data section (15)
Header data section (16)
pp; 26 DwgNo 1/20

Title Terms: DATA; ADMINISTER; METHOD; ELECTRONIC; DATA; STORAGE; MAGNETIC; DISC; FLOPPY; DISC; EMBED; INFORMATION; CONTAIN; INFORMATION; ENCRYPTION; **KEY** ; HEADER; DATA; SECTION; ELECTRONIC; WATERMARK
Derwent Class: P85; P86; T01; T03; W04
International Patent Class (Main): H04L-009/32; H04N-001/387
International Patent Class (Additional): G06F-011/30; G06F-012/14; G06T-001/00; G09C-005/00; G10K-015/02; G10L-011/00; G10L-019/00; H04L-009/08; H04N-007/08; H04N-007/081; H04N-007/16; H04N-007/167
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-D01; T01-H01B1; T03-N01; W04-F01L3

14/9/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013067179 **Image available**
WPI Acc No: 2000-239051/200021
XRPX Acc No: N00-179476

A decryption system for a broadcast data communication system such as pay-TV comprises a smart card high security decryption device, a second lower security decryption device and a device dividing messages into blocks

Patent Assignee: MINDPORT BV (MIND-N)
Inventor: RIX S P A
Number of Countries: 027 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 984630	A1	20000308	EP 98202916	A	19980901	200021	B
ZA 9905259	A	20000426	ZA 995259	A	19990818	200027	
JP 2000092045	A	20000331	JP 99242249	A	19990827	200027	

Priority Applications (No Type Date): EP 98202916 A 19980901
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 984630	A1	E	7	H04N-007/16	
ZA 9905259	A		11	H04N-000/00	
JP 2000092045	A		4	H04L-009/26	

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 984630 A1

NOVELTY - A decryption device (1), made as a smart card, has a very **high security** and holds a secret **key** for decryption. A second decryption device (2) has a **lower security** such as a personal computer. A received message is divided into blocks (3). The first block is sent to the first device and is decrypted and a clear text output is sent to the second block and is used as an initialization vector for an error-propagating block chaining method to decrypt the other blocks.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a method of distributing data within a system with a number of receivers and includes encrypting several blocks using a first encrypted block as an input vector to a block chaining method and distributing the first **key** in an encrypted message to the receivers.

USE - The decryption system is used for a broadcast data communication system such as pay-TV.

ADVANTAGE - The system renders the second decryption device as secure as the first. It prevents piracy in a pay TV system.

DESCRIPTION OF DRAWING(S) - The figure shows a simple schematic diagram of a decryption system.

Smart card decryption device (1)
Second decryption device (2)
Message dividing device (3)
pp; 7 DwgNo 1/1

Title Terms: DECRYPTER; SYSTEM; BROADCAST; DATA; COMMUNICATE; SYSTEM; PAY; TELEVISION; COMPRISE; SMART; CARD; HIGH; SECURE; DECRYPTER; DEVICE; SECOND; LOWER; SECURE; DECRYPTER; DEVICE; DEVICE; DIVIDE; MESSAGE; BLOCK
Derwent Class: T01; T04; W01; W03
International Patent Class (Main): H04L-009/26; H04N-000/00; H04N-007/16
International Patent Class (Additional): G09C-001/00; H04H-001/00; H04L-009/06; H04N-007/167
File Segment: EPI
Manual Codes (EPI/S-X): T01-D01; T01-H01B3A; T01-J12C; T04-K01; W01-A05A; W01-A05B; W03-A16C3A; W03-A16C3C
? t14/9/14,16

14/9/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012975113 **Image available**
WPI Acc No: 2000-146962/200013
XRPX Acc No: N00-108807

Multi-level security messages transmission method used in coercion resistant one time pad cryptosystem in telecommunication system

Patent Assignee: MICROSOFT CORP (MICR-N)
Inventor: CALLIGARO M P; DOUCEUR J R; THOMLINSON M W
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6021203	A	20000201	US 96763333	A	19961211	200013	B

Priority Applications (No Type Date): US 96763333 A 19961211
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6021203	A		19	H04L-009/00	

Abstract (Basic): US 6021203 A

NOVELTY - **High security** message, decoy message, random bit strings and **low security** messages are provided and one time pad (OTP) **keys** (46) and **cyphertexts** (50) are produced from the messages. The **high security** and the decoy message are embedded in the OTP **keys** and **cyphertexts** which are transmitted over the communications link to receiver (44).

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for the program for transmitting multi-level security messages.

USE - In coercion resistant one time pad cryptosystem used with sending computer and receiver computer connected via communications link in telecommunication system.

ADVANTAGE - The decoy message provides **high security** by allowing the sender or the receiver to reveal how the decoy message is hidden in the **cyphertext** and to reveal the **key** for the decoy message. Provides coercion resistance by facilitating the use of decoy messages. Provides a mechanism that can be quickly implemented with low computational overhead.

DESCRIPTION OF DRAWING(S) - The figure illustrates the block diagram of the one time pad cryptosystem.

Receiver (44)
OTP **keys** (46)
Cyphertexts (50)
pp; 19 DwgNo 4/10

Title Terms: MULTI; LEVEL; SECURE; MESSAGE; TRANSMISSION; METHOD; RESISTANCE; ONE; TIME; PAD; TELECOMMUNICATION; SYSTEM
Derwent Class: W01
International Patent Class (Main): H04L-009/00
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05; W01-A05A

14/9/16 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

012063631 **Image available**
WPI Acc No: 1998-480542/199841
Related WPI Acc No: 1996-321305; 1996-333397; 1996-412901; 1996-485825;

1996-506343; 1997-021501; 1997-363122; 1999-302138; 2000-095656; 2002-266190

XRPX Acc No: N98-374934

Monitoring and control system for security of restricted areas - over-rides code hopping algorithm **and controls system functions in response to reception of** low security **command by controller**

Patent Assignee: DIRECTED ELECTRONICS INC (DIRE-N); ISSA D (ISSA-I)

Inventor: BIRCHFIELD J W; CHEN C; ISSA D E; BIRCHFIELD J; ISSA D

Number of Countries: 061 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5798711	A	19980825	US 92886871	A	19920522	199841	B
			US 92945667	A	19920916		
			US 93112940	A	19930830		
			US 95396020	A	19950228		
			US 95396115	A	19950228		
			US 95425597	A	19950420		
			US 95460106	A	19950602		
WO 9916035	A1	19990401	WO 97US16844	A	19970919	199920	N
AU 9744303	A	19990412	AU 9744303	A	19970919	199934	N
			WO 97US16844	A	19970919		

Priority Applications (No Type Date): US 95460106 A 19950602; US 92886871 A 19920522; US 92945667 A 19920916; US 93112940 A 19930830; US 95396020 A 19950228; US 95396115 A 19950228; US 95425597 A 19950420; WO 97US16844 A 19970919; AU 9744303 A 19970919

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5798711	A		33	G06F-007/04	CIP of application US 92886871
					CIP of application US 92945667
					CIP of application US 93112940
					CIP of application US 95396020
					CIP of application US 95396115
					CIP of application US 95425597
					CIP of patent US 5432670
					CIP of patent US 5534845
WO 9916035	A1	E		G08C-017/02	

Designated States (National): AM AT AU BB BG BR BY CA CH CN CZ DE DK ES FI GB GE HU JP KE KG KP KR KZ LK LT LU LV MD MG MN MW NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN

Designated States (Regional): AT BE CH DE DK ES FI FR GB GH GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9744303	A			G08C-017/02	Based on patent WO 9916035

Abstract (Basic): US 5798711 A

The system includes a controller (35) and a remote control transmitter (25) which transmits system command comprising a code word with a fixed position word and a hopping word to the controller. The fixed position word has an identification code for controlling the controller and a channel code for issuing **high** and **low security** commands to the controller. The ID code is programmed in the controller.

A hopping **algorithm** is used for modifying the hopping code n-times in response to n-times activation of the transmitter and modifying hopping word m-times within the controller on receiving the code word from the transmitter. A bypass mode is set for bypassing the code hopping **algorithm** and for controlling system functions when controller receives **low security** command.

ADVANTAGE - Prevents cross-wording between format words and code words.

Dwg.1/10

Title Terms: MONITOR; CONTROL; SYSTEM; SECURE; RESTRICT; AREA; RIDE; CODE; HOP; **ALGORITHM** ; CONTROL; SYSTEM; FUNCTION; RESPOND; RECEPTION; LOW; SECURE; COMMAND; CONTROL
Derwent Class: T01; W05
International Patent Class (Main): G06F-007/04; G08C-017/02
File Segment: EPI
Manual Codes (EPI/S-X): T01-E04; T01-J12C; T01-S01C; W05-C03; W05-D04A1; W05-D05B
? t14/9/31,35

14/9/31 (Item 31 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

004623057
WPI Acc No: 1986-126400/198620
Related WPI Acc No: 1991-081782
XRPX Acc No: N86-093434
Magnetic card issuing method - using machine including card reader, keyboard and memory allowing issue of cards in response to entry of secret code
Patent Assignee: OMRON TATEISI ELECTRONICS CO (OMRO)
Inventor: ITO H; TAKAHASHI H; TSUCHIDA K; UEMURA Y
Number of Countries: 012 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 180948	A	19860514	EP 85113991	A	19851104	198620	B
US 4912310	A	19900327	US 88157136	A	19880210	199018	
EP 180948	B	19911218				199151	
DE 3584946	G	19920130				199206	

Priority Applications (No Type Date): JP 84233491 A 19841105; JP 84233492 A 19841105; JP 84233493 A 19841105; JP 84233494 A 19841105
Cited Patents: A3...8744; FR 2370308; GB 2118614; No-SR.Pub; US 4213118; US 4283710
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 180948	A	E	132		
Designated States (Regional): AT BE CH DE FR GB IT LI LU NL SE					
EP 180948	B				
Designated States (Regional): AT BE CH DE FR GB IT LI LU NL SE					

Abstract (Basic): EP 180948 A
The method includes use of a machine having a memory in which an initial secret code is stored. The machine further includes a card reader, and a **keyboard** . The method check whether a secret code **keyed** in by the user matches that which has been initially stored in memory. A card code is stored, both in the machine's memory, and on the card, when a card is issued in response to the entry of a valid, checked code.
USE - Dispensing magnetic, or IC/microprocessor type cards used to control access to locked areas.
Dwg.1/32
Abstract (Equivalent): EP 180948 B
A method of issuing cards by using a card issuing machine including a memory having stored therein an initial secret code, a card reader (21) and a **keyboard** (16), the method comprising: **keying** in a secret code, checking whether said a code matches a first secret code wtih a first card of a specific security level when said secret codes are found to match, characterised in that for said first card being the card (GR) of the **highest security** level above steps are preceded by

checking whether a secret code **keyed** in matches the initial secret code stored in the memory, storing in a memory a code **keyed** in for said first card with the card issuing machine and recording the associating **keyed** in code in the first card by the card reader to issue the first card when the **keyed** in secret code is found to match with said initial secret code and by **keying** in further data including said first secret code for storing it in the memory to enable the **highest** level **security** card to be used for issuing the cards of **lower** **security** level. (61pp)

Abstract (Equivalent): US 4912310 A

The method of issuing cards by using a card issuing machine with a memory with an initial secret code stored in it, a card reader and a **keyboard** , involves checking whether a secret code **keyed** in on the **keyboard** matches the initial secret code stored in the memory. When the above two secret codes are found to match, a specified secret code is stored into memory, the specified secret code being **keyed** in and associated a card with the card issuing machine the associating specified secret **keyed** -in code is recorded in the card by the card reader, and the first card is issued.

A **keyed** -in secret code of the card issued is confirmed and at least one second-type card is issued. A second secret code of one second-type card issued is confirmed, one third type card is issued.

ADVANTAGE- **High** **security** .

Title Terms: MAGNETIC; CARD; ISSUE; METHOD; MACHINE; CARD; READ; **KEYBOARD** ; MEMORY; ALLOW; ISSUE; CARD; RESPOND; ENTER; SECRET; CODE

Derwent Class: T04

International Patent Class (Additional): G06F-015/30; G06K-013/00

File Segment: EPI

Manual Codes (EPI/S-X): T04-B

14/9/35 **(Item 35 from file: 347)**

DIALOG(R)File 347:JAPIO

(c) 2004 JPO & JAPIO. All rts. reserv.

07743360 **Image available**

CERTIFYING MEDIUM CREATING DEVICE

PUB. NO.: 2003-237262 [JP 2003237262 A]
PUBLISHED: August 27, 2003 (20030827)
INVENTOR(s): FUCHITA TAKASHI
APPLICANT(s): TOSHIBA CORP
APPL. NO.: 2002-040423 [JP 200240423]
FILED: February 18, 2002 (20020218)
INTL CLASS: B42D-015/10

ABSTRACT

PROBLEM TO BE SOLVED: To provide a certifying medium creating device, which easily makes an unlocking work having a comparatively **higher** **security** level possible under the continuation of a work having a comparatively **lower** **security** level such as a data inputting work.

SOLUTION: An ID card creating device comprises a controlling part 1 and a card creating device main body 2 controlled by the controlling part. In the work having the **lower** **securing** properties such as the data inputting work or the like, a personal certification is performed by inputting a full name and a pass word through a **key** board 5 of the controlling part 1, while, in the work having the **higher** **securing** properties such as the unlocking of the lock of the card creating device main body 2 or the like, the personal certification is performed by inputting fingerprint

information from a certification information inputting part 9, resulting in performing the unlocking work of the lock of the card creating device main body 2 under the continuation of the data inputting work in the controlling part 1.

COPYRIGHT: (C)2003,JPO
?

```
File   9:Business & Industry(R) Jul/1994-2004/Apr 21
         (c) 2004  The Gale Group
File  16:Gale Group PROMT(R) 1990-2004/Apr 22
         (c) 2004 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2004/Apr 22
         (c) 2004 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2004/Apr 22
         (c)2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2004/Apr 22
         (c) 2004 The Gale Group
File 570:Gale Group MARS(R) 1984-2004/Apr 22
         (c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Apr 21
         (c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Apr 22
         (c) 2004 The Gale Group
File 649:Gale Group Newswire ASAP(TM) 2004/Apr 21
         (c) 2004 The Gale Group

Set     Items   Description
S1    4396973   KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM? OR KEY??????? ?
S2       1659   COMMON(1W)S1 OR COMMONKEY?
S3      45470   (PUBLIC OR ASYMMETRIC? OR SECRET OR SYMMETRIC OR CONVENTIO-
             NAL OR PRIVATE)(1W)S1 OR PRIVATEKEY? OR PUBLICKEY? OR SECRETK-
             EY?
S4    4412837   SECURITY OR SECURE? OR SECURING OR SECRET?
S5     225514   S4(2N)(HIGH??? ? OR MAXIMUM OR MAX OR GREAT??? ? OR MOST OR
              BEST OR OPTIMAL OR OPTIMAL OR OPTIMUM)
S6       6216   S4(2N)(OPTIMIS? OR OPTIMIZ?)
S7          1   S4(2N)(MIN()MAX OR MINMAX)
S8      25814   S4(2N)(LOW??? ? OR MINIMUM OR MIN OR SLIGHT? OR LEAST)
S9         79   S2(S)S3
S10         5   S9(S)S5:S8
S11         1   S10/1999:2004
S12         4   S10 NOT S11
S13         3   RD (unique items)
S14     18069   S1(S)S5:S6
S15      1178   S1(S)S7:S8
S16       177   S15(S)S14
S17       103   S16/1999:2004
S18        74   S16 NOT S17
S19        48   RD (unique items)
S20        48   S19 NOT S10
```

13/3,K/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05318721 Supplier Number: 48096449 (USE FORMAT 7 FOR FULLTEXT)
Secure Electronic-Mail: Return To Sender?
Willis, David
Network Computing, p108
Nov 1, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2172

... Microsoft Exchange, Eudora Pro and Netscape mailers. It uses the International Data Encryption Algorithm (IDEA) **secret - key algorithm** with 128-bit keys. IDEA is generally accepted to be much stronger and faster than Digital Encryption Standard (DES), the **most common secret - key algorithm** . In addition, PGPmail compresses text before applying encryption, reducing both storage and transmission requirements.
A...

13/3,K/2 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

04123229 SUPPLIER NUMBER: 15517239 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How to keep it a secret. (data encryption methods and how they work) (PC Tech: Tutor)(Column) (Tutorial)
Prosise, Jeff
PC Magazine, v13, n13, p315(4)
July, 1994
DOCUMENT TYPE: Tutorial ISSN: 0888-8507 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3287 LINE COUNT: 00247

...ABSTRACT: algorithm and a password. The XOR cipher, or Vernam cipher, is one of the most **common** single- **key** systems used on computers. One of the **most secure** one-key systems is the US government's Data Encryption Standard (DES) system. **Public - key** , or two-key, cryptosystems utilize a **public** encryption **key** and a **private** decryption **key** . This system makes it easy to send a message without having to send a password...

13/3,K/3 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02097007 SUPPLIER NUMBER: 19656448 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Time to spend electronic money. (e-commerce issues for businesses) (Internet/Web/Online Service Information)
Kessler, Gary; Sheppard, Steve
Network VAR, v5, n8, p65(8)
August, 1997
ISSN: 1082-8818 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 5177 LINE COUNT: 00468

... so that the same plaintext will yield different ciphertext every

time it is encrypted.

The **most** common secret key encryption scheme used today is the data encryption standard (DES), designed by IBM in the...

...rejected it; the use of 128-bit keys is under consideration at this time. Other **secret key** cryptography schemes in use today include Triple-DES (variants of DES that use either two...

20/3,K/15 (Item 2 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2004 The Gale group. All rts. reserv.

04628077 SUPPLIER NUMBER: 18734892 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Is it safe out there? (sidebar to "Secure Your Mac") (Technology Information)
Beckman, Mel
Macworld, v13, n11, p150(3)
Nov, 1996
ISSN: 0741-8647 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2183 LINE COUNT: 00180

... of your Web pages can initiate a secure session, quietly yet safely exchanging public encryption **keys** with a requesting browser and then encrypting subsequent traffic with one of three **algorithms** , DES (**least secure**), RC4-40, and RC4-128 (**most secure**). Any of these **algorithms** significantly slows Web access, so you'll only want to secure selected pages, such as...

20/3,K/35 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02132836 SUPPLIER NUMBER: 20101068 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lock down your desktops and servers with the protection of Troy. (Security First Technologies Troy) (Software Review) (Evaluation)
Cobb, Michael
Databased Web Advisor, v15, n12, p74(3)
Dec, 1997
DOCUMENT TYPE: Evaluation ISSN: 1090-6436 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1504 LINE COUNT: 00123

... files within the cache lifetime, then Troy doesn't re-compute the hash value. The **algorithm** used to calculate the hash values also affects the speed and security of Troy. During installation, you can choose one of three **algorithms** : Message Digest 5 (MD5) is the default choice, the Secure Hash **Algorithm** (SHA) is the slowest but **most secure** , and Partial MD5 the fastest but **least secure** .

The Troy Monitor can be set to run in either Enforce Verification or Advisory Verification...

20/3,K/36 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02064281 SUPPLIER NUMBER: 19413072 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The component war heats up. (ActiveX, Java becoming more alike) (Technology Information)
Lawton, George
Software Magazine, v17, n5, p51(3)
May, 1997
ISSN: 0897-8085 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2053 LINE COUNT: 00164

... want to download controls that have been signed by well-established firms, they could set **security** to the **highest** level. On the other hand,

if they want to download any applet, regardless of whether it has been signed, they would set **security** at its **lowest** setting. The **keys** for certifying software are managed by VeriSign Inc., Mountain View, Calif., a spin-off of...
? t20/3,k/37-38

20/3,K/37 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01704094 SUPPLIER NUMBER: 16255880 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Network Information Service+. (SunSoft Inc's network software for providing nameservices) (Product Announcement)
Noor, Arshad
UNIX Review, v12, n11, p47(5)
Oct, 1994
DOCUMENT TYPE: Product Announcement ISSN: 0742-3136 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3062 LINE COUNT: 00235

... both before performing any operation on the namespace.
NIS+ authentication has three levels: 0 (the **least secure**), 1, and 2 (the **most secure**). At level 0, there is no authentication - everyone has privileges to do anything in the...

...the uid. At level 2, the authentication is the strictest. Level 2 uses 192-bit **keys** with the Diffie-Hellmann cryptography scheme to encrypt and decrypt passwords over a network. The...

20/3,K/38 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01525654 SUPPLIER NUMBER: 12340158 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Responses to NIST's proposal. (National Institute of Standards and Technology) (includes related article about the digital signature standard specifications) (Technical)
Communications of the ACM, v35, n7, p41(14)
July, 1992
DOCUMENT TYPE: Technical ISSN: 0001-0782 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5671 LINE COUNT: 00440

... authorities, or users with very valuable data, must use very long keys to achieve the **highest** possible **security** level. Other users, with reduced security requirements and/or more stringent performance requirements, will use shorter **keys** . Trying to make one-size-fit-all results either in unacceptably **low security** for all users (because all certificates will be suspect) or unacceptably poor performance for some...
?

```
File 256:SoftBase:Reviews,Companies&Prods. 82-2004/Mar
         (c)2004 Info.Sources Inc
File   2:INSPEC 1969-2004/Apr W2
         (c) 2004 Institution of Electrical Engineers
File   6:NTIS 1964-2004/Apr W3
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2004/Apr W2
         (c) 2004 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2004/Apr W3
         (c) 2004 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2004/Mar
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/Apr W3
         (c) 2004 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2004/Apr W1
         (c)2004 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2004/Apr W1
         (c) 2004 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Mar
         (c) 2004 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2004/Apr 22
         (c) 2004 The Gale Group
File 144:Pascal 1973-2004/Apr W2
         (c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File 266:FEDRIP 2004/Feb
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2004/Apr 17
         (c) 2004 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
File 603:Newspaper Abstracts 1984-1988
         (c)2001 ProQuest Info&Learning

Set     Items   Description
S1    2747803   KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM? OR KEY??????? ?
S2       1752   COMMON(1W)S1 OR COMMONKEY?
S3      26783   (PUBLIC OR ASYMMETRIC? OR SECRET OR SYMMETRIC OR CONVENTIO-
             NAL OR PRIVATE)(1W)S1 OR PRIVATEKEY? OR PUBLICKEY? OR SECRETK-
             EY?
S4    1445659   SECURITY OR SECURE? OR SECURING OR SECRET?
S5      29435   S4(2N)(HIGH??? ? OR MAXIMUM OR MAX OR GREAT??? ? OR MOST OR
              BEST OR OPTIMAL OR OPTIMAL OR OPTIMUM)
S6        904   S4(2N)(OPTIMIS? OR OPTIMIZ?)
S7          3   S4(2N)(MIN()MAX OR MINMAX)
S8       8752   S4(2N)(LOW??? ? OR MINIMUM OR MIN OR SLIGHT? OR LEAST)
S9        224   S2 AND S3
S10        24   S9 AND S5:S8
S11      1062   S5:S6(15N)S1
S12       139   S7:S8(15N)S1
S13        16   S11 AND S12
S14        38   S10 OR S13
S15        20   S14/1999:2004
S16        18   S14 NOT S15
S17        10   RD (unique items)
```

17/7/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

6110259 INSPEC Abstract Number: B9901-6120D-040, C9901-1260C-039
Title: Constructing identity-based key distribution systems over elliptic curves
Author(s): Sakazaki, H.; Okamoto, E.; Mambo, M.
Author Affiliation: Sch. of Inf. Sci., Japan Adv. Inst. of Sci. & Technol., Ishikawa, Japan
Journal: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences vol.E81-A, no.10 p.2138-43
Publisher: Inst. Electron. Inf. & Commun. Eng,
Publication Date: Oct. 1998 Country of Publication: Japan
CODEN: IFESEX ISSN: 0916-8508
SICI: 0916-8508(199810)E81A:10L.2138:CIBD;1-P
Material Identity Number: P710-98011
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Theoretical (T)
Abstract: A key distribution system is a system in which users securely generate a **common key** . One kind of identity-based key distribution system was proposed by E. Okamoto [1993]. Its security depends on the difficulty of factoring a composite number of two large primes like RSA **public - key** cryptosystem. Another kind of identity-based key distribution system was proposed by K. Nyberg and R.A. Rueppel [1993]. Its security depends on the difficulty of the discrete logarithm problem. On the other hand, Koblitz and Miller described how a group of points on an elliptic curve over a finite field can be used to construct a **public key** cryptosystem. In 1997, we proposed an ID-based key distribution system over an elliptic curve, as well as those over the ring Z/nZ. Its security depends on the difficulty of factoring a composite number of two large primes. We showed that this system over an elliptic curve is more suitable for the implementation than those over the ring Z/nZ. In this paper, we apply the Nyberg-Rueppel ID-based key distribution system to an elliptic curve. It provides relatively small block size and **high security** . This **public key** distribution system can be efficiently implemented. However the Nyberg-Rueppel's scheme requires relatively large data transmission. As a solution to this problem, we improve the scheme. This improved scheme is very efficient since data transferred for the **common key** generation is reduced to half of those in the Nyberg-Rueppel's scheme. (16 Refs)
Subfile: B C
Copyright 1998, IEE

17/7/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

6078089 INSPEC Abstract Number: B9812-6120B-095, C9812-6130S-074
Title: Design of secure authenticated key distribution protocols
Author(s): Xu Shengbo; Tian Jianbo; Wang Xinmei
Author Affiliation: Sch. of Commun. Eng., Xidian Univ., Xi'an, China
Journal: Journal of Xidian University vol.25, no.4 p.495-9
Publisher: Xidian Univ,
Publication Date: Aug. 1998 Country of Publication: China
CODEN: XDKXEP ISSN: 1001-2400
SICI: 1001-2400(199808)25:4L.495:DSAD;1-P
Material Identity Number: D328-98009
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Theoretical (T)

Abstract: The confidentiality and authenticity of cryptology have been thoroughly analyzed and some rules have been proposed for designing secure authenticated key distribution protocols. We have analyzed the authentication protocol designed by R.M. Needham and M.D. Schroder (1978) and found its drawback according to the above rules. Finally, we have designed a new authenticated **key** distribution protocol, which has **high security** and **low** complexity. (10 Refs)

Subfile: B C

Copyright 1998, IEE

17/7/3 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2004 Institution of Electrical Engineers. All rts. reserv.

5992160 INSPEC Abstract Number: B9809-6120B-094, C9809-6130S-054

Title: The application of ID-based key distribution systems to an elliptic curve

Author(s): Sakazaki, H.; Okamoto, E.; Mambo, M.

Author Affiliation: Sch. of Inf. Sci., Adv. Inst. of Sci. & Technol., Ishikawa, Japan

Conference Title: Information Security. First International Workshop, ISW'97. Proceedings p.335-44

Editor(s): Okamoto, E.; Davida, G.; Mambo, M.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1998 Country of Publication: Germany xii+356 pp.

ISBN: 3 540 64382 6 Material Identity Number: XX98-00997

Conference Title: Information Security. First International Workshop, ISW'97 Proceedings

Conference Date: 17-19 Sept. 1997 Conference Location: Ishikawa, Japan

Language: English Document Type: Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: A key distribution system is a system in which users securely generate a **common key**0 . One kind of identity-based key distribution system was proposed by Okamoto (1993). Its security depends on the difficulty of factoring a composite number of two large primes like RSA **public - key** cryptosystem. Another kind of identity-based key distribution system was proposed by Nyberg and Rueppel (1993). Its security depends on the difficulty of the discrete logarithm problem. On the other hand, Koblitz and Miller described how a group of points on an elliptic curve over a finite field can be used to construct a **public key** cryptosystem. In 1997, we proposed an ID-based key distribution system over an elliptic curve, as well as over a ring Z/nZ. Its security depends on the difficulty of factoring a composite number of two large primes. We showed that the system is more suitable for the implementation on an elliptic curve than on a ring Z/nZ. In this paper, we apply the Nyberg-Rueppel ID-based key distribution system to an elliptic curve. It provides relatively small block size and **high security** . This **public key** scheme can be efficiently implemented. However the scheme requires relatively large data transmission. As a solution to this problem, we improve the scheme. The improved scheme is very efficient since the data transferred for generation of a **common key** is reduced to half of the previous one. (14 Refs)

Subfile: B C

Copyright 1998, IEE

17/7/4 (Item 4 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2004 Institution of Electrical Engineers. All rts. reserv.

4801884 INSPEC Abstract Number: C9412-6130S-019
Title: Cryptographic security: origins, development, and applications
Author(s): Jamieson, R.; Hayes, J.B.
Author Affiliation: Sch. of Inf. Syst., New South Wales Univ., Sydney, NSW, Australia
Journal: IS Audit & Control Journal vol.3 p.48-57
Publication Date: 1994 Country of Publication: USA
CODEN: IACJET ISSN: 0885-0445
U.S. Copyright Clearance Center Code: 0885-0445/94/$2.50+25
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)
Abstract: The article presents an overview of the origins of cryptography, provides some insights into the development of cryptography by reviewing a selection of codes and ciphers, and provides some examples of their use. In summary, the effectiveness of any encryption scheme depends on the following factors: frequency of use; communications **security** ; **low** error propagation; **high** physical lsecurity ; the encryption **algorithm** ; and adequate **key** management. (27 Refs)
Subfile: C

17/7/5 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

4501438
Title: Healthy security at children's hospital
Author(s): Harowitz, S.L.
Journal: Security Management vol.37, no.8 p.42-4, 46, 48
Publication Date: Aug. 1993 Country of Publication: USA
CODEN: SECME6 ISSN: 0145-9406
Language: English Document Type: Journal Paper (JP)
Treatment: Applications (A)
Abstract: At the Children's National Medical Center, the challenges faced by security are as wide ranging as the problems brought to the hospital's doors daily by its several thousand visitors. The entire building is secured with a proximity card access system, chosen to replace a more limited magnetic stripe card system about two years ago. The access card system is supplemented by **keypads** for security research labs that work with infectious materials and other areas that demand extra **security** . **High** -resolution, **low** -light, pan/tilt cameras and passive infrared motion detectors are located in all hospital stairways, in elevator lobbies and at outside entrances. The electronic security system's effectiveness is evidenced by the decreasing number of incidents of theft and vandalism since it has been installed. (0 Refs)
Subfile: D

17/7/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

01779151 INSPEC Abstract Number: B82002555
Title: A new approach to communications security
Author(s): Spielvogel, J.
Conference Title: MECOM'81. 2nd Middle East Electronic Communications Show and Conference p.14 pp.
Publisher: Arabian Exhibition Management, Birmingham, UK
Publication Date: 1981 Country of Publication: UK 452 pp.

Zurich//Switzerland/ (REPRINT); ETH Zurich,Swiss Fed Inst Technol, Dept Comp Sci,CH-8092 Zurich//Switzerland/
, 1997, V1294, P307-321
ISSN: 0302-9743 Publication date: 19970000
Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, D-14197 BERLIN, GERMANYADVANCES IN CRYPTOLOGY - CRYPTO'97, PROCEEDINGS
Series: LECTURE NOTES IN COMPUTER SCIENCE
Language: English Document Type: ARTICLE
Abstract: Privacy amplification allows two parties Alice and Bob knowing a partially secret string S to extract, by communication over a public channel, a shorter, **highly secret** string S '. Bennett, Brassard, Crepeau, and Maurer showed that the length of S ' can be almost equal to the conditional Renyi entropy of S given an opponent Eve's knowledge. All previous results on privacy amplification assumed that Eve has access to the public channel but is passive or, equivalently, that messages inserted by Eve can be detected by Alice and Bob. In this paper we consider privacy amplification secure even against active opponents. First it is analyzed under what conditions information-theoretically secure authentication is possible even though the **common key** is only partially secret. This result is used to prove that privacy amplification can be secure against an active opponent and that the size of S ' can be almost equal to Eve's min-entropy about S minus 2n/3 if S is an n-bit string. Moreover, it is shown that for sufficiently large on privacy amplification is possible when Eve's min-entropy about S exceeds only n/2 rather than 2n/3.

17/7/9 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus
(c)2004 Japan Science and Tech Corp(JST). All rts. reserv.

03833104 JICST ACCESSION NUMBER: 98A0986943 FILE SEGMENT: JICST-E
Information Theory and Its Applications. Constructing Identity-Based Key Distribution Systems over Elliptic Curves.
SAKAZAKI H (1); OKAMOTO E (1); MAMBO M (1)
(1) Japan Advanced Inst. Sci. And Technol., Ishikawa-ken, Jpn
IEICE Trans Fundam Electron Commun Comput Sci(Inst Electron Inf Commun Eng)
, 1998, VOL.E81-A,NO.10, PAGE.2138-2143, TBL.2, REF.16
JOURNAL NUMBER: F0699CAT ISSN NO: 0916-8508
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3 681.3.02-759
LANGUAGE: English COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: A key distribution system is a system in which users securely generate a **common key** . One kind of identity-based key distribution system was proposed by E. Okamoto 1!. Its security depends on the difficulty of factoring a composite number of two large primes like RSA **public - key** cryptosystem. Another kind of identity-based key distribution system was proposed by K. Nyberg, R.A. Rueppel 7!. Its security depends on the difficulty of the discrete logarithm problem. On the other hand, Koblitz and Miller described how a group of points on an elliptic curve over a finite field can be used to construct a **public key** cryptosystem. In 1997, we proposed an ID-based key distribution system over an elliptic curve 14!, as well as those over the ring Z/nZ. Its security depends on the difficulty of factoring a composite number of two large primes. We showed that this system over an elliptic curve is more suitable for the implementation than those over the ring Z/nZ 14!. In this paper, we apply the Nyberg-Rueppel ID-based key distribution system 7! to an elliptic curve. It provides

relatively small block size and **high security** . This **public key** distribution system can be efficiently implemented. However the Nyberg-Rueppel's scheme requires relatively large data transmission. As a solution to this problem, we improve the scheme. This improved scheme is very efficient since data transferred for the **common key** generation is reduced to half of those in the Nyberg-Rueppel's scheme. (author abst.)

17/7/10 (Item 1 from file: 266)
DIALOG(R)File 266:FEDRIP
Comp & dist by NTIS, Intl Copyright All Rights Res. All rts. reserv.

00190103
IDENTIFYING NO.: 0325207 AGENCY CODE: NSF
ITR: A Hardware/Compiler Co-Design Approach to Software Protection
PRINCIPAL INVESTIGATOR: Simha, Rahul
PERFORMING ORG.: George Washington University, Department of Computer Science, Washington, DC 20052
PROJECT MONITOR: Landwehr, Carl E.
SPONSORING ORG.: National Science Foundation, CNS, 4201 Wilson Boulevard , Arlington, Virginia 22230
DATES: 20030901 TO 20040831 FY : 2003 FUNDS: $523,620 (500000)
SUMMARY: ITR: A Compiler-Hardware Co-Design Approach to Software Protection PI's: Rahul Simha, Bhagi Narahari, Alok Choudhary, Nasir Memon Abstract: The growing area of software protection aims to address the problems of code understanding and code tampering along with related problems such as authorization. This project will combine novel techniques in the areas of compilers, architecture, and software security to provide a new, efficient, and tunable approach to some problems in software protection. The goal is to address a broad array of research issues that will ultimately enable design tools such as compilers to assist system designers in managing the tradeoffs between security and performance. The main idea behind the proposed approach is to hide code sequences (keys) within instructions in executables that are then interpreted by supporting FPGA (Field Programmable Gate Array) hardware to provide both a "language" (the code sequences) and a "virtual machine within a machine" (the FPGA) that will allow designers considerable flexibility in providing software protection. Thus, by using long sequences and PKI to exchange a secret key with the FPGA while also encrypting the executable with that secret **key** , a system can be positioned at the **high - security** (but **low** -performance) end of the spectrum. Similarly, as will be explained in the proposal, by using shorter sequences and selective encryption, one can achieve high-performance with higher security than is possible with systems that rely only on obscurity.
?

File 696:DIALOG Telecom. Newsletters 1995-2004/Apr 21
(c) 2004 The Dialog Corp.
File 15:ABI/Inform(R) 1971-2004/Apr 21
(c) 2004 ProQuest Info&Learning
File 98:General Sci Abs/Full-Text 1984-2004/Apr
(c) 2004 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2004/Apr W3
(c) 2004 ProQuest
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2004/Apr 21
(c) 2004 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 369:New Scientist 1994-2004/Apr W2
(c) 2004 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
File 20:Dialog Global Reporter 1997-2004/Apr 22
(c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Apr 19
(c) 2004 McGraw-Hill Co. Inc
File 634:San Jose Mercury Jun 1985-2004/Apr 21
(c) 2004 San Jose Mercury News
File 647:CMP Computer Fulltext 1988-2004/Apr W2
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Apr W2
(c) 2004 IDG Communications

Set	Items	Description
S1	4293224	KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM? OR KEY??????? ?
S2	948	COMMON(1W)S1 OR COMMONKEY?
S3	23617	(PUBLIC OR ASYMMETRIC? OR SECRET OR SYMMETRIC OR CONVENTIONAL OR PRIVATE)(1W)S1 OR PRIVATEKEY? OR PUBLICKEY? OR SECRETKEY?
S4	7979040	SECURITY OR SECURE? OR SECURING OR SECRET?
S5	194342	S4(2N)(HIGH??? ? OR MAXIMUM OR MAX OR GREAT??? ? OR MOST OR BEST OR OPTIMAL OR OPTIMAL OR OPTIMUM)
S6	3196	S4(2N)(OPTIMIS? OR OPTIMIZ?)
S7	1	S4(2N)(MIN()MAX OR MINMAX)
S8	29363	S4(2N)(LOW??? ? OR MINIMUM OR MIN OR SLIGHT? OR LEAST)
S9	66	S2(S)S3
S10	2	S9(S)S5:S8
S11	0	S10/1999:2004
S12	2	S10 NOT S11
S13	2	RD (unique items)
S14	10453	S5:S6(S)S1
S15	1065	S7:S8(S)S1
S16	135	S15(S)S14
S17	93	S16/1999:2004
S18	42	S16 NOT S17
S19	39	RD (unique items)

19/3,K/4 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

01416554 00067541
The component war heats up
Lawton, George

Software Magazine v17n5 PP: 51-54 May 1997
ISSN: 0897-8085 JRNL CODE: SMG
WORD COUNT: 1950

...TEXT: want to download controls that have been signed by well-established firms, they could set **security** to the **highest** level. On the other hand, if they want to download any applet, regardless of whether it has been signed, they would set **security** at its **lowest** setting. The keys for certifying software are managed by VeriSign Inc., Mountain View, Calif., a spin-off of...

...the first place. The hacker would not necessarily even have to apply for their own **key** . As Authenticode technology grows in acceptance, it is not unreasonable to assume that some **keys** may be stolen and traded by hackers. They may be physically copied or electronically pilfered as they are sent down the Internet. It is noteworthy that the **keys** used by well-established software vendors require a physical encryption "dongle," or hardware **key** , that plugs into the back of the PC. Since the dongle can be physically locked in a safe, and its absence quickly noted by the vendor, this system affords a **higher** level of **security** than that offered by applets signed by individuals.

Java applets do not have this same...

19/3,K/8 (Item 6 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

00923607 95-72999
Network Information Service+
Noor, Arshad
UNIX Review v12n11 PP: 47-54 Oct 1994
ISSN: 0742-3136 JRNL CODE: UXR
WORD COUNT: 2858

...TEXT: both before performing any operation on the namespace.

NIS+ authentication has three levels: 0 (the **least secure**), 1, and 2 (the **most secure**). At level 0, there is no authentication--everyone has privileges to do anything in the...

... the uid. At level 2, the authentication is the strictest. Level 2 uses 192-bit **keys** with the Diffie-Hellmann cryptography scheme to encrypt and decrypt passwords over a network. The...

19/3,K/10 (Item 8 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)
(c) 2004 ProQuest Info&Learning. All rts. reserv.

00621994 92-37096
Who Holds the Keys? Debating Data Encryption Standards
Lyons, John W.; Anderson, John C.; Hellman, Martin E.; Rivest, Ronald L.
Communications of the ACM v35n7 PP: 32-54 Jul 1992
ISSN: 0001-0782 JRNL CODE: ACM
WORD COUNT: 14387

...TEXT: authorities, or users with very valuable data, must use very long keys to achieve the **highest** possible **security** level. Other users, with

reduced security requirements and/or more stringent performance requirements, will use shorter **keys** . Trying to make one-size-fit-all results either in unacceptably **low security** for all users (because all certificates will be suspect) or unacceptably poor performance for some... ?

File 347:JAPIO Nov 1976-2003/Dec(Updated 040402)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200426
(c) 2004 Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2004/Apr W02
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040415,UT=20040408
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	952	AU='NISHIMURA T':AU='NISHIMURA T RICOH TOTTORI SOFTWARE TECHN CO LT'
S2	157	AU='NISHIMURA TAKUYA'
S3	114	AU='IITSUKA H':AU='IITSUKA HIROYUKI'
S4	1566	AU='YAMADA M':AU='YAMADA M NTT INTELLECTUAL PROPERTY CENTER'
S5	265	AU='YAMADA MASAZUMI'
S6	77	AU='GOTOH S'
S7	7	AU='GOTOH SHOICHI'
S8	40	AU='TAKECHI H':AU='TAKECHI H YAMAHA HATSUDOKI KABUSHIKI KAISHA'
S9	104	AU='TAKECHI HIDEAKI':AU='TAKECHI HIDEAKI ROOM 201 11 10 KOMATSU 4 CHOME'
S10	11	AU='USUKI N'
S11	10	AU='USUKI NAOSHI'
S12	488897	KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM?
S13	4677	S12(3N)COMMON OR COMMONKEY?
S14	3085	S1:S11
S15	6	S14 AND S13

15/5/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01445406
COPYRIGHT PROTECTIVE SYSTEM, TRANSMITTER, RECEIVER, BRIDGE DEVICE, COPYRIGHT PROTECTIVE METHOD, MEDIUM, AND PROGRAM
URHEBESRECHTSCHUTZSYSTEM, UBERTRAGER, EMPFANGER, BRUCKENGERAT. URHEBERRECHTSCHUTZ-VERFAHREN, MITTEL UND PROGRAMM
SYSTEME ET PROCEDE DE PROTECTION DES DROITS D'AUTEUR, EMETTEUR, RECEPTEUR, DISPOSITIF D'INTERFACE DE CONNEXION, SUPPORT ET PROGRAMME ASSOCIES
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Yamada, Masazumi , 11-14-301,Ikutamacho Tennoji-ku, Osaka-shi Osaka 543-0071, (JP)
Iitsuka, Hiroyuki , 6-25-6, Kisaichi, Katano-shi Osaka 576-0033, (JP)
Usuki, Naoshi , 26-12,Hashimotoisoku, Yawata-shi Kyo to 614-8331, (JP
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1235389 A1 020828 (Basic)
WO 2002030054 020411
APPLICATION (CC, No, Date): EP 2001967691 010917; WO 2001JP8034 010917
PRIORITY (CC, No, Date): JP 20002985 000929
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
INTERNATIONAL PATENT CLASS: H04L-012/28; G06F-013/00

ABSTRACT EP 1235389 A1
In the case that a bridge unit is connected to a network such as an IEEE 1394 bus, the desire of copyright holders for limitation on the number of apparatuses that can receive a signal cannot be met.
The invention is characterized by providing at least one reception unit, or more, that receives and utilizes data requiring copyright protection, connected to a network and by providing a transmission unit 20 for transmitting data requiring copyright protection to a reception unit by utilizing a network, wherein the transmission unit 20 has an authentication means 23 on the transmission side for carrying out authentication for a reception unit and an authentication number counting means 24 for counting the authentication number that is the number of the authentications carried out by the authentication means 23 on the transmission side while the reception unit has an authentication means on the reception side for carrying out authentication for the authentication means on the transmission side and wherein the above authentication number is limited.
ABSTRACT WORD COUNT: 169
NOTE:
Figure number on first page: 0001

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020828 A1 Published application with search report
Examination: 020828 A1 Date of request for examination: 20020627
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200235	3742
SPEC A	(English)	200235	29004
Total word count - document A			32746
Total word count - document B			0
Total word count - documents A + B			32746

15/5/2 (Item 2 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01203740

COMPUTER AND PROGRAM RECORDED MEDIUM
RECHNER UND PROGRAMMAUFGENOMMENES MEDIUM
ORDINATEUR ET SUPPORT COMPORTANT UN PROGRAMME ENREGISTRE

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
TAKECHI, Hideaki , 6-17-407, Kamishinden 3-chome, Toyonaka-shi, Osaka 533-0004, (JP)
YAMADA, Masazumi , 6-24-10, Kinda-cho, Moriguchi-shi, Osaka 570-0011, (JP)
IITSUKA, Hiroyuki , 6-25-6, Kisaichi, Katano-shi Osaka 576-0033, (JP)
NISHIMURA, Takuya , 3-9-18-F, Matsuzaki-cho Abeno-ku, Osaka-shi Osaka 545-0053, (JP)
KUNO, Yoshiki, 14-26-204, Oeda-nishimachi, Moriguchi-shi, Osaka 570-0054, (JP)
GOTOH, Shoichi , 6-45-710, Unobe 2-chome, Ibaraki-shi, Osaka 567-0042, (JP
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721)

, Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1083480 A1 010314 (Basic)
WO 0050989 000831
APPLICATION (CC, No, Date): EP 904054 000221; WO 00JP956 000221
PRIORITY (CC, No, Date): JP 9943870 990222
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: G06F-009/06
CITED REFERENCES (WO A):
EP 875813 A2
WO 9641468 A1
DAVID AUCSMITH.: 'Gyaku kaiseki ya kaihen kara soft wo mamoru tanpa ' resistant ' Software gijutsu no syousai' NIKKEI ELECTRONICS, vol. 706, 05 January 1998, (TOKYO), pages 209 - 220
'DVD, PC ni noru software fukugou no kagi wo nigiru fusei copy boushi gijyutsu no medo' NIKKEI ELECTRONICS, no. 696, 18 August 1997, (TOKYO), pages 110 - 119
NATSUME MATSUZAKI, HIDESHI ISHIHARA, TAKAHISA HUKUSHIMA.: 'DVD copyright protection system' THE INSTITUT OF IMAGE INFORMATION AND TELEVISION ENGINEERS, TECHNICAL REPORT, vol. 21, no. 31, 22 May 1997, (TOKYO), pages 15 - 19
NATSUME MATSUZAKI, MAKOTO TATEBAYASHI, HIDESHI ISHIHARA, TAKAHISA HUKUSHIMA.: 'DVD copyright protection system' NATIONAL TECHNICAL REPORT, vol. 43, no. 3, 18 June 1997, (TOKYO), pages 118 - 122
MASAKAZU MATSUYAMA, TAKATOSHI MATSUI, YUKIO MATSUURA, EIKI TAKAHASHI.: 'DVD-rom drive tousai PC CF-200DV' NATIONAL TECHNICAL REPORT, vol. 43, no. 3, 18 June 1997, (TOKYO), pages 31 - 35;

ABSTRACT EP 1083480 A1
The problem to be solved is that once copyright claimed AV data is passed to application software, the application software can freely process the AV data for recording, etc., defeating the purpose of copyright protection. The invention provides a computer which comprises a system section 12 and an application software section 13, and which takes in copyright claimed, encrypted data via a digital interface 1 for processing therein, wherein the system section 12 judges that the application software section 13 is legitimate application software for the protection of copyright, and if the application software is a legitimate one, the system section 12 passes a key for the encrypted data to the application software section 13.
ABSTRACT WORD COUNT: 116
NOTE:
Figure number on first page: 1
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 001025 A1 International application. (Art. 158(1))
Application: 001025 A1 International application entering European phase
Application: 010314 A1 Published application with search report
Examination: 010314 A1 Date of request for examination: 20001208
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200111	564
SPEC A	(English)	200111	9470
Total word count - document A			10034
Total word count - document B			0
Total word count - documents A + B			10034

15/5/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

01081390

DIGITAL AV DATA TRANSMITTING UNIT, DIGITAL AV DATA RECEIVING UNIT, DIGITAL AV DATA TRANSMITTING/RECEIVING UNIT, AND MEDIUM

UBERTRAGUNGS-, EMPFANGSEINHEIT UND MEDIUM FUR DIGITALE AUDIOVISUELLE DATEN

UNITE DE TRANSMISSION DE DONNEES AUDIOVIDEO (AV) NUMERIQUES, UNITE DE RECEPTION DE DONNEES NUMERIQUES AV, UNITE DE TRANSMISSION/RECEPTION DE DONNEES AV ET SUPPORT

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)

INVENTOR:
NISHIMURA, Takuya , 3-9-18-F, Matsuzaki-cho Abeno-ku, Osaka-shi Osaka 545-0053, (JP)
IITSUKA, Hiroyuki , 6-25-6, Kisaichi, Katano-shi Osaka 576-0033, (JP)
YAMADA, Masazumi , 6-24-10, Kinda-cho, Moriguchi-shi Osaka 570-0011, (JP)
GOTOH, Shoichi , 5-4-204, Myoukenzaka, Katano-shi Osaka 576-0021, (JP)
TAKECHI, Hideaki , 11-10-201, Komatsu 4-chome Higashiyodogawa-ku, Osaka-shi Osaka 533-0004, (JP)
USUKI, Naoshi , 26-12, Hashimoto Isoku, Yawata-shi Kyoto 614-8331, (JP

LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 977436 A1 000202 (Basic)
WO 9941910 990819
APPLICATION (CC, No, Date): EP 99902852 990208; WO 99JP533 990208
PRIORITY (CC, No, Date): JP 9831847 980213; JP 98151586 980601; JP 98224825 980807
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04N-007/16; H04L-009/00

ABSTRACT EP 977436 A1

A digital AV data transmitting unit comprises a data importance judging section for judging the importance of digital AV data, a transmitting-side multiple authentication rule storage section stored with multiple kinds of authentication rules, a transmitting-side authentication selecting section for selecting one kind of rules from the transmitting-side multiple authentication rule storage section, and a transmitting-side authenticating section for carrying out authentication based on the selected authentication rules. A digital AV data receiving unit comprises an authentication requesting section for making an authentication request, a receiving-side multiple authentication rule storage section stored with the same authentication rules as those stored in the transmitting-side multiple authentication rule storage section, a receiving-side authentication selecting section for selecting the predetermined authentication rules selected by the transmitting-side authentication selecting section from the receiving-side multiple authentication rule storage section, and a receiving-side authenticating section for carrying out authentication based on the authentication rules selected on the receiving side.

ABSTRACT WORD COUNT: 154

NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Search Report: 000503 A1 Date of drawing up and dispatch of supplementary:search report 20000320
Application: 20000202 A1 Published application with search report

Application: 991020 A1 International application. (Art. 158(1))
Examination: 20000322 A1 Date of request for examination: 20000118
Application: 991020 A1 International application entering European phase
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200005	4510
SPEC A	(English)	200005	16009
Total word count - document A			20519
Total word count - document B			0
Total word count - documents A + B			20519

15/5/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01075047
METHOD AND SYSTEM FOR DATA RECORDING / REPRODUCING, APPARATUS FOR RECORDING/REPRODUCING, AND MEDIA FOR RECORDING PROGRAM
VERFAHREN UND SYSTEM ZUR AUFZEICHNUNG /WIEDERGABE VON DATEN, VORRICHTUNG ZUR AUFZEICHUNG/WIEDERGABE UNDAUFZEICHUNGSMEDIUM
APPAREIL, PROCEDE ET SYSTEME D'ENREGISTREMENT / REPRODUCTION DE DONNEES, ET SUPPORTS D'ENREGISTREMENT DE PROGRAMME
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
YAMADA, Masazumi , 6-24-10, Kinda-cho Moriguchi-shi, Osaka 570-0011, (JP)
IITSUKA, Hiroyuki , 6-25-6, Kisaichi Katano-shi, Osaka 576-0033, (JP)
GOTO, Shoichi, 5-4-204, Myokenzaka Katano-shi, Osaka 576-0021, (JP)
TAKECHI, Hideaki Room 201 11-10, Komatsu 4-chome , Higashiyodogawa-ku, Osaka-shi Osaka 533-0004, (JP
LEGAL REPRESENTATIVE:
Schuster, Thomas, Dipl.-Phys. (52981), Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 989557 A1 000329 (Basic)
WO 9938164 990729
APPLICATION (CC, No, Date): EP 99900674 990125; WO 99JP292 990125
PRIORITY (CC, No, Date): JP 9812474 980126; JP 9827572 980209
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: G11B-020/10; H04N-005/91

ABSTRACT EP 989557 A1
A data recording/reproducing method wherein encrypted digital data obtained by subjecting digital data to first encrypting by using a contents key and encrypted contents key obtained by subjecting the contents key to second encrypting are recorded on a recording medium, the encrypted digital data and the encrypted contents key, having been recorded, are reproduced, and the encrypted digital data is decrypted by using the contents key obtained by decrypting the encrypted contents key, thereby to obtain the digital data.
ABSTRACT WORD COUNT: 80
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 20000329 A1 Published application with search report

Application: 990929 A1 International application. (Art. 158(1))
Examination: 20000329 A1 Date of request for examination: 19991129
Application: 990929 A1 International application entering European phase

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200013	3447
SPEC A	(English)	200013	19139
Total word count - document A			22586
Total word count - document B			0
Total word count - documents A + B			22586

15/5/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01021364
Data transmission method, data transmission system and program recording medium
Datenubertragungsverfahren und -system sowie Programmaufzeichnungsmedium
Procede de transmission de donnees, systeme de transmission de donnees et support d'enregistrement de programme

PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Iitsuka, Hiroyuki , 6-25-6, Kisaichi, Katano-shi, Osaka 576-0033, (JP)
Yamada, Masazumi , 6-24-10, Kinda-cho, Moriguchi-shi, Osaka 570-0011, (JP)
Takechi, Hideaki , 4-11-10-201, Komatsu, Higashiyodogawa-ku, Osaka-shi, Osaka 533-0004, (JP)
Matsuzaki, Natsume, 1-6-7-803, Aomadani Nishi, Mino-shi, Osaka 562-0023, (JP
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 913975 A2 990506 (Basic)
EP 913975 A3 031119
APPLICATION (CC, No, Date): EP 98120512 981029;
PRIORITY (CC, No, Date): JP 97297614 971029
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06

ABSTRACT EP 913975 A2
The data transmission system can substantially prohibit illegal copy of real data since the encryption key applied to transmitted data is changed depending on copy management information, thereby the real data being decrypted and recorded with a key different from the original key when the copy management information is tampered. Thus, the transmitted data can be further securely protected than in the prior art.
ABSTRACT WORD COUNT: 65
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Search Report: 031119 A3 Separate publication of the search report

Application: 990506 A2 Published application (Alwith Search Report ;A2without Search Report)
Examination: 040331 A2 Date of request for examination: 20040202
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9918	1784
SPEC A	(English)	9918	8959
Total word count - document A			10743
Total word count - document B			0
Total word count - documents A + B			10743

15/5/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01005277
DATA TRANSFER METHOD
DATENTRANSFERVERFAHREN
PROCEDE DE TRANSFERT DE DONNEES
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216880), 1006, Ohaza Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
NISHIMURA, Takuya , 6-1-105, Myokenzaka Katano-shi, Osaka 576-0021, (JP)
IITSUKA, Hiroyuki , 6-25-6, Kisaichi Katano-shi, Osaka 576-0033, (JP)
YAMADA, Masazumi , 6-24-10, Kinda-cho Moriguchi-shi, Osaka 570-0011, (JP
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 978965 A1 000209 (Basic)
WO 9848543 981029
APPLICATION (CC, No, Date): EP 98917616 980422; WO 98JP1837 980422
PRIORITY (CC, No, Date): JP 97106995 970424
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-012/40; H04L-009/00
CITED PATENTS (WO A): JP 61260735 A ; JP 61081043 A ; JP 1307341 A ; JP 1181349 A ; JP 9205421 A

ABSTRACT EP 978965 A1
A data transfer method which eliminates erroneous operation of conventional devices not supporting encryption when copy-protected AV information is encrypted and sent on the IEEE 1394 bus. Synchronous data transferred through isochronous communication contains i) encryption identification information for indicating encryption of actual data and ii) actual data. Only the actual data is encrypted. Encryption identification information indicating encryption status of actual data in synchronous data is sent together with actual data from the sending device. A receiving device detecting encryption of actual data from this encryption identification information requests for decrypting information to the sending device. The receiving device decrypts the actual data using decrypting information received from the sending device according to this request.
ABSTRACT WORD COUNT: 117
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 20000209 A1 Published application with search report
Application: 990331 A1 International application (Art. 158(1))

Examination: 20000209 A1 Date of request for examination: 19991021
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200006	1067
SPEC A	(English)	200006	7245
Total word count - document A			8312
Total word count - document B			0
Total word count - documents A + B			8312

a un certain nombre de tels dispositifs commandes par cle, chaque cle etant associee a un motif d'identite pour ce meme dispositif. Le dispositif d'acces portatif comporte un modele memorise qui comprend une empreinte digitale de l'utilisateur autorise associe a un code de verification. Lorsque l'utilisateur autorise applique son doigt sur le dispositif d'acces portatif, le code de verification est renvoye, ce qui permet de verifier l'utilisateur. Si le dispositif d'acces recoit ensuite un identificateur de dispositif commande par cle qui correspond a un autre identificateur se trouvant dans la memoire, la cle d'acces associee est recuperee et envoyee au dispositif commande par cle pour autoriser l'acces a l'utilisateur.

Legal Status (Type, Date, Text)
Publication 20030612 A1 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... it wants the access device 14 to send a verification code and receive a temporary **key** for encrypting the access **keys** prior to transmission and to send a " **low security** " indicator, or no security indicator, when it wants the access device 14 to follow the described 200 **low security** option.

A **high security** option is for the access **keys** to be encrypted in the access device 14. To accomplish this option, on enrolment, as...

30/5,K/13 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00792836 **Image available**
A PORTABLE COMMUNICATION APPARATUS HAVING A MAN-MACHINE INTERFACE AND A METHOD FOR ITS OPERATION
APPAREIL DE COMMUNICATION PORTATIF DOTE D'UNE INTERFACE HOMME-MACHINE ET SON PROCEDE DE FONCTIONNEMENT
Patent Applicant/Assignee:
TELEFONAKTIEBOLAGET LM ERICSSON (publ), S-126 25 Stockholm, SE, SE (Residence), SE (Nationality)
Inventor(s):
KIESSLING Johan, Rodabergsbrinken 16, S-113 30 Stockholm, SE,
ARWALD Jan, Drevkarlstigen 1, S-192 53 Stockholm, SE,
NILSSON Bernt, Olmegatan 3A, S-652 30 Karlstad, SE,
SAXEN Benny, Kyrkvardsvagen 32, S-665 33 Kil, SE,
Legal Representative:
STROM Tore (et al) (agent), Strom & Gulliksson AB, P.O. Box 4188, S-203 13 Malmo, SE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200126401 A1 20010412 (WO 0126401)
Application: WO 2000SE1807 20000919 (PCT/WO SE0001807)
Priority Application: SE 993560 19991001; SE 20001996 20000526
Designated States: AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM DZ EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04Q-007/32
International Patent Class: H04L-029/06; H04Q-007/38
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 4282

English Abstract
A portable communication apparatus (1) has a man-machine interface (2-5, 21), a controller (23), an operating system (25), a local storage device (24) for storing a first application (26, 27), a secure resource (29) which is only accessible from the operating system, and a wireless interface (30-32) for connecting the portable communication apparatus to a remote device. The man-machine interface provides interaction between a user of the portable communication apparatus and the first application when executed by the controller and the operating system. The man-machine interface also provides interaction between the user and a second application (28) originating from the remote device. The operating system (25) and only the operating system can provide a security indicator (22) through the man-machine interface (2-5, 21). The security indicator represents a secure connection between the secure resource (29) and the one of the first and second applications (26-28), which currently uses the man-machine interface.

French Abstract
Un appareil de communication portatif (1) comprend une interface homme-machine (2-5, 21), un controleur (23), un systeme d'exploitation (25), et un dispositif de stockage local (24) pour le stockage d'une premiere application (26, 27), une ressource protegee (29) seulement accessible par le systeme d'exploitation et une interface sans fil (30-32) pour la connexion de l'appareil de communication portatif a un dispositif eloigne. L'interface homme-machine permet l'interaction entre un utilisateur de l'appareil de communication portatif et la premiere application, lorsqu'elle est executee par le controleur et le systeme d'exploitation. L'interface homme-machine permet egalement l'interaction entre l'utilisateur et une deuxieme application (28) provenant du dispositif eloigne. Seul le systeme d'exploitation (25) peut fournir un indicateur de securite (22) par l'intermediaire de l'interface homme-machine (2-5, 21). L'indicateur de securite represente une connexion protegee entre la ressource protegee (29) et une des applications parmi la premiere ou la deuxieme application (26-28), qui utilise ponctuellement l'interface homme-machine.

Legal Status (Type, Date, Text)
Publication 20010412 A1 With international search report.
Publication 20010412 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20010712 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... then advantageously be

indicated graphically as indicated by the icon 22a in Fig.

3. Three **key** symbols in the icon 22a represent a **high** -level **security** , whereas two **key** symbols represent a medium-level security, only one **key** symbol represents a **low** -level **security** and, finally, no **key** symbol at all represents no security.

The security indicator (22h in Fig. 7) may also...

30/5,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00766059 **Image available**
QUERY INTERFACE TO POLICY SERVER
INTERFACE D'INTERROGATION VERS SERVEUR DE REGLES
Patent Applicant/Assignee:
INTERNET DYNAMICS INC, 3717 E. Thousand Oaks Boulevard, Westlake Village, CA 91362, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HANNEL Clifford Lee, 3178 Futura Point, Thousand Oaks, CA 91362, US, US (Residence), US (Nationality), (Designated only for: US)
MAY Anthony Allan, 6644 Glade Avenue #217, Woodland Hills, CA 91303, US, US (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
NELSON Gordon E, 57 Central Street, P.O. Box 782, Rowley, MA 01969, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200079434 A1 20001228 (WO 0079434)
Application: WO 2000US17078 20000621 (PCT/WO US0017078)
Priority Application: US 99140417 19990622
Designated States: AU JP SG US
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-017/30
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 54190

English Abstract
A scalable access filter that is used together with others like it in a virtual private network to control access by users at clients in the network to information resources provided by servers in the network. Each access filter use a local copy of an access control data base (3845) to determine whether an access request is made by a user. Each user belongs to one or more user groups and each information ressource belongs to one or more information sets. Access is permitted or denied according to access policies which define access in terms of the user groups and information sets. The first access filter in the path performs the access check, encrypts and authenticates the request; the other access filters in the path do not repeat the access check. The interface used by applications to determine whether a user has access to an entity is now an SQL query. The policy server (3811) assembles the information needed for the response to the query from various information sources, including source external to the policy server.

French Abstract

L'invention concerne un filtre d'acces scalaire utilise avec d'autres filtres similaires dans un reseau prive virtuel afin de controler l'acces des utilisateurs a des clients du reseau pour obtenir des ressources d'informations fournies par des serveurs sur le reseau. Chaque filtre d'acces utilise une copie locale d'une base de donnees de controle d'acces (3845) pour determiner si la demande d'acces est effectuee par un utilisateur. Chaque utilisateur appartient a au moins un groupe d'utilisateurs et chaque ressource d'informations appartient a au moins un ensemble d'informations. L'acces est autorise ou refuse en fonction des politiques d'acces qui definissent l'acces en terme des groupes d'utilisateurs et des ensembles d'informations. Le premier filtre d'acces dans la voie effectue la verification d'acces, decrypte, et authentifie la demande, les autres filtres d'acces dans la voie ne repetent pas la verification d'acces. L'interface utilisee par les applications pour determiner si un utilisateur a acces a une entite est alors une demande SQL. Le serveur de regles (3811) assemble les informations requises pour la reponse a la demande emanant de plusieurs sources d'informations, y compris une source externe audit serveur.

Legal Status (Type, Date, Text)
Publication 20001228 A1 With international search report.
Examination 20010802 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... the order of identification techniques. The administrator of the access filter likewise orders the cryptographic **algorithms** available in the VPN from **most secure** to **least secure** and relates the ordered trust levels to the ordered
33
cryptographic **algorithms** and orders the network paths employed in VPN 201 and relates the ordered trust levels...

30/5,K/18 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00754009 **Image available**
A METHOD OF PROVIDING SECURE TRANSMISSION FOR FACSIMILE DATA MODEM SIGNALS
PROCEDE POUR LA TRANSMISSION PROTEGEE DE SIGNAUX DE MODEM DE DONNEES ET DE FAC-SIMILE

Patent Applicant/Assignee:
AMIK INC, 10580 S.W. McDonald Street, Suite 202, Tigard, OR 97224, US, US (Residence), US (Nationality)
Inventor(s):
COLLETT Gordon C, 2155 N.W. Chrystal Drive, McMinnville, OR 97128, US
GALE Gary A, 47665 N.W. Deer Court, Box 5018, Manning, OR 97125, US
Legal Representative:
ROSENBERG Gerald B, 285 Hamilton Avenue, Suite 520, Palo Alto, CA 94301, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200067409 A2 20001109 (WO 0067409)
Application: WO 2000US11573 20000428 (PCT/WO US0011573)
Priority Application: US 99303521 19990430
Designated States: AU CA IN MX
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04K
Publication Language: English

Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 8910

English Abstract
A method of operating a security device to secure the transmission of data between authorized modems and against interception byA method of operating a security device to secure the transmission of data between authorized modems and against interception by an unauthorized modem. The modems each implement a defined protocol that includes negotiation and data transport portions of a communications session that is conducted over a network utilizing signals selectively occurring in a plurality of frequency channels. The security device includes a first interface coupleable to a modem to exchange first predetermined signals occurring in a first plurality of frequency channels and a second interface coupleable to a network to exchange second predetermined signals occuring in a second plurality of frequency channels. A signal processor is coupled between the first and second interfaces, to implement a bi-directional conversion of the signals between the first and second plurality of frequency channels by frequency shifting the first and second predetermined signals between the first and second pluralities of frequency channels. Further, the security device can provide for a first frequency shift of greater than a predetermined frequency tolerance specified by the defined protocol for a first portion of said communications session and a second frequency shift for a second portion of the communications session.

French Abstract
L'invention concerne un procede d'exploitation d'un dispositif de securite concu pour proteger la transmission de donnees entre des modems autorises et pour empecher l'interception par un modem non autorise. Les modems mettent en oeuvre chacun un protocole qui comprend des parties de negociation et de transport de donnees d'une session de communications menee a bien sur un reseau utilisant des signaux apparaissant selectivement dans plusieurs voies de frequence. Le dispositif de securite comporte une premiere interface pouvant etre couplee a un modem pour l'echange de premiers signaux predetermines apparaissant dans une premiere pluralite de voies de frequence, et une seconde interface pouvant etre couplee a un reseau pour l'echange de seconds signaux predetermines apparaissant dans une seconde pluralite de voies de frequence. Un processeur de signal est couple entre les premiere et seconde interfaces, de sorte qu'il assure un conversion bidirectionnelle des signaux entre la pluralite de voies de frequence, par deplacement de la frequence des premiers et seconds signaux predetermines entre les premiere et seconde pluralites de voies de frequence. Par ailleurs, le dispositif de securite peut permettre un premier deplacement de frequence superieur a une tolerance de frequence predeterminee specifiee par le protocole pour une premiere partie de ladite session de communication, et un deuxieme deplacement de frequence pour une deuxieme partie de la session de communication.

Legal Status (Type, Date, Text)

Publication	20001109	A2 Without international search report and to be republished upon receipt of that report.
Search Rpt	20010125	Late publication of international search report
Examination	20010329	Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:

Detailed Description

Detailed Description
... security mode, or may operate in the clear or any available security mode; (3) a **low** -security encoding **key** ; and (4) a **high** - **security** **key** seed value. In alternate embodiments of the present invention, the code selector 1 64 may...

...be supported in a preferred method of operation in accordance with the present invention. The **low** - **security** process path preferably uses a fixed security **key** , while the **high** - **security** process path includes a **key** exchange. In initial embodiments, the **high** - **security** device is not interoperable with **low** - security devices unless pre-preemptively set to emulate a low-security device by a manual switch...Also, the inquiry/response exchange may be expanded to allow for adaptive transitions between different **high** and **low** - **security** levels and, potentially, the use of different **key** exchange and permutation **algorithms** . Nonstandard DTMF tones, or other tones altogether, can also be utilized in the inquiry/response...

30/5,K/21 (Item 21 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00537506 **Image available**
GENERALIZED POLICY SERVER
SERVEUR DE PROCEDURE GENERALISEE
Patent Applicant/Assignee:
INTERNET DYNAMICS INC,
HANNEL Clifford L,
LIPSTONE Laurence R,
SCHNEIDER Davis S,
Inventor(s):
HANNEL Clifford L,
LIPSTONE Laurence R,
SCHNEIDER Davis S,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200000879 A2 20000106 (WO 0000879)
Application: WO 99US14585 19990628 (PCT/WO US9914585)
Priority Application: US 9891130 19980629
Designated States: AU JP SG US AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: G06F-015/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 35547

English Abstract
A policy system includes the policy server (2617); a policy database (2619) which located at policy decision point (2723); the access/response entity (2603); resource server (2711); policy message (2725) and policy enforcement point (2721). System connected through public network (2702) or internal network (103). The access filter (107, 203, 403) control access by use a local copy of an access control data base to determine

whether an access request made by a user. Changes made by administrators in the local copies are propagated to all of the other local copies. Access is permitted or denied according to of access policies (307) which define access in terms of the user groups (Fig 9-12) and information sets (Fig 13A-18). The rights of administrators are similarly determined by administrative policies (Fig 23A-C). Access is further permitted only if the trust levels of the network by which is made by the sufficient access (Fig 25-29). A policy server component of the access filter has been separated from the access filter and the policies have been generalized to permit administrators of the policy server to define new types of actions and new types of entities. Policies may now further have specifications for time intervals during which the policies are in force and the entities may be associated with attributes that specify how the entity is to be used when the policy applies.

French Abstract

La presente invention concerne un filtre d'acces evolutif, utilise ensemble avec d'autres filtres semblables dans un reseau prive virtuel, destine a controler l'acces, par des utilisateurs chez des clients du reseau, aux ressources d'information mises a disposition par des serveurs du reseau. Chaque filtre d'acces utilise une copie locale d'une base de donnees de controle d'acces afin de determiner si une requete d'acces est effectuee par un utilisateur. Des changements effectues par des administrateurs dans des copies locales sont propages a toutes les autres copies locales. Chaque utilisateur appartient a un ou a plusieurs groupes d'utilisateurs et chaque ressource d'information appartient a un ou plusieurs ensembles d'informations. Un acces est permis ou refuse selon des procedures d'acces qui le definissent en termes de groupes d'utilisateurs et d'ensembles d'informations. Les droits des administrateurs sont determines de maniere semblable par des procedures administratives. En outre un acces est permis seulement si les niveaux de confiance d'un mode d'identification de l'utilisateur et du chemin dans le reseau, par lequel est effectue l'acces, sont suffisants en regard du niveau de sensibilite de la ressource d'information. Si necessaire, le filtre d'acces code automatiquement la demande a l'aide d'une methode de codage dont le niveau de confiance est suffisant. Le premier filtre d'acces dans le chemin met en oeuvre le test d'acces, code et authentifie la demande ; les autres filtres d'acces du chemin ne repetent pas le test d'acces. Un composant de serveur de procedure de filtre d'acces a ete separe du filtre d'acces et les procedures ont ete generalisees afin de permettre aux administrateurs du serveur de procedure de definir de nouveaux types d'actions et de nouveaux types d'entites pour lesquelles des procedures peuvent etre mises en place. Des procedures peuvent maintenant comporter, en plus, des specifications de durees pendant lesquelles les procedures font autorite, et les entites peuvent etre associees avec des attributs qui specifient comment l'entite doit etre utilisee lorsque la procedure s'applique.

Fulltext Availability:
Detailed Description

Detailed Description
... the order of identification techniques. The administrator of the access filter likewise orders the cryptographic **algorithms** available in the VPN from **most secure** to **least secure** and relates the ordered trust levels to the ordered cryptographic **algorithms** and orders the network paths employed in VPN 201 and relates the ordered trust levels...

? t27/5,k/2-3

27/5,K/2 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00484683 **Image available**
EMBEDDED CODE HOPPING SYSTEM WITH BYPASS MODE
SYSTEME DE CODE DE SAUTS INTEGRE AVEC MODE EVITEMENT
Patent Applicant/Assignee:
DIRECTED ELECTRONICS INC,
ISSA Darrell,
Inventor(s):
ISSA Darrell,
BIRCHFIELD Jerry,
CHEN Charles,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9916035 A1 19990401
Application: WO 97US16844 19970919 (PCT/WO US9716844)
Priority Application: WO 97US16844 19970919
Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK ES FI GB GE HU JP KE KG KP KR KZ LK LT LU LV MD MG MN MW NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN GH KE LS MW SD SZ UG ZW AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: G08C-017/02
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 16115

English Abstract
An area monitoring and controlling system (29) ensures that the security of commands is maintained by employing "fixed" and "hopping" code words in command transmissions, and that certain functions which are executable from a remote transmitter (25) are assigned as " **low security** " and are executed in conjunction with a "bypass mode" to bypass the hopping **algorithm** which is necessary to execute the " **high security** " functions.

French Abstract
L'invention concerne un systeme (29) de surveillance et de controle de zone qui garantit que la securite des ordres est maintenue par l'utilisation de mots de code "fixe" et "de sauts" dans les transmissions d'ordres et que certaines fonctions qui peuvent etre executee a partir d'un emetteur (25) a distance sont affectees avec un critere "basse securite" et sont executees avec un "mode evitement" pour contourner l'algorithme de sauts qui est necessaire pour l'execution des fonctions "haute securite".
Fulltext Availability:
Claims

English Abstract
...and that certain functions which are executable from a remote transmitter (25) are assigned as " **low security** " and are executed in conjunction with a "bypass mode" to bypass the hopping **algorithm** which is necessary to execute the " **high security** " functions.

Claim
... said controller, said
identification code programmed in said controller,

and a channel code for issuing **high** and **low** **security** commands to said controller;
d) a hopping **algorithm** for modifying said hopping code of said transmitter n-times in response to n-times...to a system controller;
b) programming said identification code within said controller;
C) assigning a **high** **security** or a **low** **security** to said channel code;
d) programming a hopping **algorithm** into said transmitter and said controller, each having a 0-times modified initial hopping word...to a system controller;
b) programming said identification code within said controller;
c) assigning a **high** **security** or a **low** **security** to said channel code;
d) programming a hopping **algorithm** into said transmitter and said controller, each having a 0-times modified initial hopping word...

27/5,K/3 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00354420
TOKENLESS IDENTIFICATION SYSTEM FOR AUTHORIZATION OF ELECTRONIC TRANSACTIONS AND ELECTRONIC TRANSMISSIONS
SYSTEME D'IDENTIFICATION SANS JETONS
Patent Applicant/Assignee:
SMART TOUCH L L C,
Inventor(s):
HOFFMAN Ned,
PARE David F,
LEE Jonathan A,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9636934 A1 19961121
Application: WO 96US7185 19960517 (PCT/WO US9607185)
Priority Application: US 95442895 19950517
Designated States: AM AT AU BB BG BR BY CA CH CN CZ DE DK ES FI GB GE HU JP KE KG KP KR KZ LK LT LU LV MD MG MN MW MX NO NZ PL PT RO RU SD SE SI SK TJ TT UA UZ VN KE LS MW SD SZ UG AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: G06K-009/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 45133

English Abstract
A tokenless identification system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously (1). It can be networked to act as a full or partial intermediary between other independent computer systems (3), or maybe the sole computer systems carrying out all necessary executions.

French Abstract

Un systeme et un procede d'identification sans jetons sont principalement fondes sur une comparaison correlative d'un echantillon biometrique unique, tel qu'une empreinte digitale ou un enregistrement de voix, obtenus directement d'un utilisateur inconnu, un echantillon biometrique authentifie du meme type etant obtenu et stocke au prealable (1). On peut le mettre en reseau de sorte qu'il serve d'intermediaire total ou partiel entre d'autres systemes informatiques independants (3), ou bien seuls les systemes informatiques effectuent toutes les operations necessaires.

Fulltext Availability:
Claims

Claim
... initial key as a series of DES
encrypt/decrypt/encrypt cycles to generate the transaction **key** .
For additional security, two Base **Key** Lists are maintained, one for **low security** BIA devices and one for **high security** devices. The MDM chooses which Base **Key** List to use depending on the security level of the device.
1 14 Database Schema...
?

? t30/5,k/5,10,13-14,18,21

30/5,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00822168
TOKENLESS IDENTIFICATION SYSTEM
IDENTIFIKATIONSSYSTEM OHNE IDENTITATSMARKER
SYSTEME D'IDENTIFICATION SANS JETONS
PATENT ASSIGNEE:
Indivos Corporation, (3944030), 155 Grand Avenue, Suite 1050, Oakland, California 94612, (US), (Proprietor designated states: all)
INVENTOR:
HOFFMAN, Ned, Suite 12, 46 Shattuck Square, Berkeley, CA 94704, (US)
PARE, David, F., Suite 12, 46 Shattuck Square, Berkeley, CA 94704, (US)
LEE, Jonathan, A., Suite 12, 46 Shattuck Square, Berkeley, CA 94704, (US)
LEGAL REPRESENTATIVE:
Stoner, Gerard Patrick et al (59901), MEWBURN ELLIS York House 23 Kingsway, London WC2B 6HP, (GB)
PATENT (CC, No, Kind, Date): EP 912959 A1 990506 (Basic)
EP 912959 A1 990506
EP 912959 B1 031112
WO 96036934 961121
APPLICATION (CC, No, Date): EP 96916498 960517; WO 96US7185 960517
PRIORITY (CC, No, Date): US 442895 950517
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: LT
INTERNATIONAL PATENT CLASS: G06K-009/00; G07C-009/00; G07F-007/10
CITED PATENTS (EP B): EP 651357 A; WO 94/10659 A; US 5191611 A; US 5229764 A; US 5335288 A; US 5386104 A
NOTE:
No A-document published by EPO
LEGAL STATUS (Type, Pub Date, Kind, Text):

Examination:	010627 A1	Date of dispatch of the first examination report: 20010511
Application:	970319 A1	International application (Art. 158(1))
Grant:	031112 B1	Granted patent
Assignee:	020116 A1	Transfer of rights to new applicant: Indivos Corporation (3944030) 155 Grand Avenue, Suite 1050 Oakland, California 94612 US
Change:	020717 A1	Title of invention (German) changed: 20020527
Change:	020717 A1	Title of invention (English) changed: 20020527
Application:	990506 A1	Published application (A1with Search Report ;A2without Search Report)
Search Report:	990506 A1	Drawing up of a supplementary European search report: 990209
Examination:	990506 A1	Date of filing of request for examination: 971216

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200346	1179
CLAIMS B	(German)	200346	1087
CLAIMS B	(French)	200346	1374
SPEC B	(English)	200346	40147
Total word count - document A			0
Total word count - document B			43787
Total word count - documents A + B			43787

30/5,K/10 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

01019029 **Image available**

PORTABLE DEVICE AND METHOD FOR ACCESSING DATA KEY ACTUATED DEVICES

DISPOSITIF PORTATIF ET PROCEDE D'ACCES A DES DISPOSITIFS COMMANDES PAR DES CLES DE DONNEES

Patent Applicant/Assignee:
BIOSCRYPT INC, Suite 500, 5450 Explorer Drive, Mississauga, Ontario L4W 5M1, CA, CA (Residence), CA (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
HOLLINGSHEAD Dennis W, Suite 200, 1220 Sheppard Avenue East, Toronto, Ontario M2K 2S5, CA, CA (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
FETHERSTONHAUGH & CO (agent), Attention: Ronald d. Faggetter, Suite 1500, Box 111, 438 University Avenue, Toronto, Ontario M5G 2K8, CA,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200349042 A1 20030612 (WO 0349042)
Application: WO 2001CA1736 20011206 (PCT/WO CA0101736)
Priority Application: WO 2001CA1736 20011206
Parent Application/Grant:
Related by Continuation to: US 9878396 19980513 (CIP)
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: G07C-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 3638

English Abstract
Data key actuated devices such as high security doors are modified so that they periodically transmit an identity pattern. An authorized user is provided with a portable access device storing keys for a number of such key actuated devices, with each key associated with an identity pattern for that device. The portable access device has a stored template comprising a fingerprint of the authorized user combined with a verification code. When the authorized user applies their fingerprint to the portable access device, the verification code is returned which allows verification of the user. If the access device then receives a key actuated device identifier matching one in storage, the associated access key is retrieved and transmitted to the key actuated device to allow access to the user.

French Abstract
Des dispositifs commandes par des cles de donnees, tels que des portes de haute securite, sont modifies de maniere a ce qu'ils envoient periodiquement un motif d'identite. Un utilisateur autorise est equipe d'un dispositif d'acces portatif qui garde en memoire des cles destinees

Application: 010801 A2 Published application without search report
Examination: 010801 A2 Date of request for examination: 20010410
Change: 011010 A2 International Patent Classification changed: 20010817
Search Report: 011010 A3 Separate publication of the search report
Examination: 030514 A2 Date of dispatch of the first examination report: 20030328
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200131	207
SPEC A	(English)	200131	21556
Total word count - document A			21763
Total word count - document B			0
Total word count - documents A + B			21763

...INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION production of pirated disks can be prevented.
To overcome Problem 3, both a first-generation **cipher** with a **low** degree of **security** and a second-generation **cipher** with a **high** degree of **security** , each enciphering the position information with a digital signature, are prerecorded on a medium and...preserving compatibility between different generations can be obtained. Furthermore, a combination of three kinds of ciphers of different generations, such as **secret key cipher** , **low - security** public **key cipher** , and **high - security** public **key cipher** , may also be used.

INDUSTRIAL APPLICABILITY
As described above, in the present invention, for example...

23/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00779891
MARKING GENERATING APPARATUS, METHOD OF FORMING LASER MARKING ON OPTICAL DISK, REPRODUCING APPARATUS, OPTICAL DISK AND OPTICAL DISK PRODUCING METHOD
GERAT ZUR ERZEUGUNG EINER MARKIERUNG, VERFAHREN ZUR ERZEUGUNG EINER LASERMARKIERUNG AUF EINER OPTISCHEN PLATTE, OPTISCHE PLATTE UND VERFAHREN ZU DEREN HERSTELLUNG
APPAREIL GENERATEUR DE MARQUAGE, PROCEDE DE FORMATION D'UN MARQUAGE AU LASER SUR DISQUE OPTIQUE, APPAREIL DE REPRODUCTION, DISQUE OPTIQUE ET PROCEDE DE PRODUCTION DE DISQUE OPTIQUE
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
OSHIMA, Mitsuaki, 115-3, Minamitatsumi-cho, Katsura, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
GOTOH, Yoshiho, Room 201, 9-17, Higashinkahama 4-chome, Jyoto-ku, Osaka-shi, Osaka 536, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721) , Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 741382 A1 961106 (Basic)
EP 741382 A1 970702
EP 741382 B1 011010

WO 9616401 960530
APPLICATION (CC, No, Date): EP 95938017 951116; WO 95JP2339 951116
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247 951009
DESIGNATED STATES: DE; FR; GB
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1120777 (EP 2001108949)
INTERNATIONAL PATENT CLASS: G11B-007/00; G11B-020/10; G11B-023/30; G11B-013/04; G11B-019/06; G11B-007/09; G11B-020/00; **G06F-001/00**
CITED PATENTS (EP B): EP 553545 A; DE 4308680 A; JP 2044448 A; JP 5266576 A ; JP 7325712 A; JP 61190734 A; JP 63046541 A; JP 63164043 A; NL 9101358 A

ABSTRACT EP 741382 A1
An object of the present invention is to provide a marking forming apparatus, a method of forming a laser marking on an optical disk, a reproduction apparatus, an optical disk, and a method of manufacturing an optical disk, capable of providing a greatly improved copy prevention capability as compared to prior known construction. To achieve this object, in the optical disk of the invention, for example, a marking is formed by a laser on a reflective film of a disk holding data written thereon and at least position information of the marking or information concerning the position information is written on the disk in an encrypted form or with a digital signature appended thereto. (see image in original document)
ABSTRACT WORD COUNT: 139
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Change:	010606 A1	Application number of divisional application (Article 76) changed: 20010418
Application:	960828 A	International application (Art. 158(1))
Oppn None:	021002 B1	No opposition filed: 20020711
Grant:	011010 B1	Granted patent
Application:	961106 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	970108 A1	Date of filing of request for examination: 961112
Change:	970611 A1	Obligatory supplementary classification (change)
Search Report:	970702 A1	Drawing up of a supplementary European search report: 970514
Examination:	990922 A1	Date of dispatch of the first examination report: 19990804

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	1884
CLAIMS B	(English)	200141	1217
CLAIMS B	(German)	200141	1189
CLAIMS B	(French)	200141	1383
SPEC A	(English)	EPAB96	21543
SPEC B	(English)	200141	21174
Total word count - document A			23431
Total word count - document B			24963
Total word count - documents A + B			48394

...INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION production of pirated disks can be prevented.
To overcome Problem 3, both a first-generation **cipher** with a **low**

degree of **security** and a second-generation **cipher** with a **high** degree of **security** , each enciphering the position information with a digital signature, are prerecorded on a medium and...preserving compatibility between different generations can be obtained. Furthermore, a combination of three kinds of **ciphers** of different generations, such as **secret key cipher** , **low - security** public **key cipher** , and **high - security** public **key cipher** , may also be used.

INDUSTRIAL APPLICABILITY
As described above, in the present invention, for example...

...SPECIFICATION production of pirated disks can be prevented.
To overcome Problem 3, both a first-generation **cipher** with a **low** degree of **security** and a second-generation **cipher** with a **high** degree of **security** , each enciphering the position information with a digital signature, are prerecorded on a medium and...preserving compatibility between different generations can be obtained. Furthermore, a combination of three kinds of **ciphers** of different generations, such as **secret key cipher** , **low - security** public **key cipher** , and **high - security** public **key cipher** , may also be used.

INDUSTRIAL APPLICABILITY
As described above, in the present invention, for example...

23/5,K/16 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00762698 **Image available**
SECURE CONTROL OF SECURITY MODE
CONTROLE SUR DU MODE DE SECURISATION
Patent Applicant/Assignee:
GENERAL INSTRUMENT CORPORATION, 101 Tournament Drive, Horsham, PA 19044, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
QIU Xin, 101 Tournament Drive, Horsham, PA 19044, US, US (Residence), US (Nationality)
MORONEY Paul, 10529 Harvest View Way, San Diego, CA 92128, US, US (Residence), US (Nationality)
SPRUNK Eric J, 3411 Western Springs Road, Olivenhain, CA 92024, US, US (Residence), US (Nationality)
Legal Representative:
KULAS Charles J, Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200076117 A1 20001214 (WO 0076117)
Application: WO 2000US15870 20000608 (PCT/WO US0015870)
Priority Application: US 99138163 19990608; US 2000576516 20000523
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **H04L-009/00**

International Patent Class: **H04N-007/167**
Publication Language: English
Filing Language: English
Fulltext Availability:
  Detailed Description
  Claims
Fulltext Word Count: 5676

English Abstract
  A system to change security levels is used to change the level of security used in a secured processing system. The system uses a status indicator to designate the security level being implemented. The security level can be upgraded to allow a higher level of security to be implemented with relative ease. However, in order to change from a higher level of security to a lower level of security, an authorization code is utilized to confirm that the change in security is authorized.

French Abstract
  La presente invention concerne un systeme permettant de modifier les niveaux de securisation, utilise pour modifier le niveau de securisation dans un systeme de traitement securise. Ce systeme utilise un indicateur d'etat permettant d'indiquer le niveau de securisation mis en oeuvre. On peut hausser le niveau de securisation de facon a permettre de mettre en oeuvre assez facilement un niveau de securisation plus eleve. Neanmoins, on utilise un code d'autorisation pour confirmer que la modification relative a la securisation est autorisee, lorsque l'on souhaite passer d'un niveau de securisation eleve a un niveau inferieur.

Legal Status (Type, Date, Text)
Publication 20001214 A1 With international search report.
Publication 20001214 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.
Examination 20010426 Request for preliminary examination prior to end of 19th month from priority date
Main International Patent Class: **H04L-009/00**
International Patent Class: **H04N-007/167**
Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... to be compromised because it would become 1 0 secured according to a more secure **algorithm** . However, if an attacker is able to cause a shift to a **low** level of **security** from a **high** level of **security** , the attacker has made the process of breaking the code that much easier. Therefore, there...value is detected, it is tested to determine whether it indicates a change from a **low** level **security** **algorithm** to a **higher** level **security** **algorithm** (e.g., by changing from a "O" to a "I") 132. If this is the...from an outside source, e.g., the transmitter. The processor stores the code for the **lower** level **security** **algorithm** 282 and code for the **higher** level **security** **algorithm** 278 in its internal memory. The Security Level Status Indicator (SLSI) 286 is stored in...

Claim
... authenticated and protected against a replay attack.

18 The method of claim I wherein a **lower** level of **security** is nonpublic **Key** mode, wherein a **higher** level of **security** is a public

Key mode, the method
further comprising:
continuing operation of the system in the public Key mode...

23/5,K/17 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00754060 **Image available**
AN APPARATUS FOR PROVIDING SECURE TRANSMISSION FOR FACSIMILE DATA MODEM SIGNALS
APPAREIL ASSURANT UNE TRANSMISSION SECURISEE DE SIGNAUX DE FAC-SIMILE SUR DES MODEMS DE DONNEES
Patent Applicant/Assignee:
AMIK INC, 10580 S.W. McDonald Street, Suite 202, Tigard, OR 97224, US, US (Residence), US (Nationality)
Inventor(s):
COLLETT Gordon C, 2155 N.W. Chrystal Drive, McMinnville, OR 97128, US
GALE Gary A, 47665 N.W. Deer Court, Box 5018, Manning, OR 97125, US
Legal Representative:
ROSENBERG Gerald B, 285 Hamilton Avenue, Suite 520, Palo Alto, CA 94301, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200067467 A1 20001109 (WO 0067467)
Application: WO 2000US11729 20000428 (PCT/WO US0011729)
Priority Application: US 99303203 19990430
Designated States: AU CA IN MX
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04N-001/44**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9303

English Abstract
A security device operates to secure the transmission of data between authorized modems and against interception by an unauthorized modem. The modems each implement a defined protocol that includes negotiation and data transport portions of a communications session that is conducted over a network utilizing signals selectively occurring in a plurality of frequency channels. The security device includes a first interface coupleable to a modem to exchange first predetermined signals occurring in a first plurality of frequency channels and a second interface coupleable to a network to exchange second predetermined signals occurring in a second plurality of frequency channels. A signal processor is coupled between the first and second interfaces, to implement a bi-directional conversion of the signals between the first and second plurality of frequency channels by frequency shifting the first and second predetermined signals between the first and second pluralities of frequency channels. Further, the security device can provide for a first frequency shift of greater than a predetermined frequency tolerance specified by the defined protocol for a first portion of said communications session and a second frequency shift for a second portion of the communications session.

French Abstract
L'invention concerne un dispositif de securite qu'on met en oeuvre pour securiser la transmission de signaux de donnees entre des modems

autorises et empecher leur interception par un modem non autorise. Chaque modem met en oeuvre un protocole defini qui inclut une partie negociation et une partie transport dans une session de communications ouverte dans un reseau utilisant des signaux achemines selectivement dans plusieurs voies de frequence. Le dispositif de securite comprend une premiere interface pouvant etre couplee a un modem pour echanger une premiere serie de signaux predetermines achemines dans un premier groupe de voies de frequence, et une deuxieme interface pouvant etre reliee a un reseau pour echanger une deuxieme serie de signaux predetermines achemines dans un deuxieme groupe de voies de frequence. Un processeur de signaux est couple entre la premiere et la deuxieme interfaces pour effectuer une conversion bidirectionnelle de signaux entre le premier et le deuxieme groupes de voies de frequence, par deplacement de la frequence de la premiere et de la deuxieme series de signaux predetermines entre le premier et le deuxieme groupes de voies de frequence. Le dispositif de securite peut en outre assurer, d'une part, un premier deplacement de frequence ayant une plus grande tolerance qu'une frequence predeterminee specifiee par le protocole defini d'une premiere partie de ladite session de communications, d'autre part, un deuxieme deplacement de frequence pour une deuxieme partie de la session de communications.

Legal Status (Type, Date, Text)
Publication 20001109 A1 With international search report.
Examination 20010607 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04N-001/44**
Fulltext Availability:
Detailed Description

Detailed Description
... security mode, or may operate in the clear or any available security mode; (3) a **low** -security encoding **key** ; and (4) a **high - security key** seed value. In alternate embodiments of the present invention, the code selector 164 may also...

...be supported in a preferred method of operation in accordance with the present invention. The **low - security** process path preferably uses a fixed security **key** , while the **high - security** process path includes a **key** exchange. In initial embodiments, the **high - security** device is not interoperable with **low - security** devices unless pre-preemptively set to emulate a low-security device by a manual switch...Also, the inquiry/response exchange may be expanded to allow for adaptive transitions between different **high** and **low - security** levels and, potentially, the use of different **key** exchange and permutation **algorithms** . Nonstandard DTMF tones, or other tones altogether, can also be utilized in the inquiry/response...

23/5,K/18 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00754059 **Image available**
SYSTEM OF PROVIDING SECURE TRANSMISSION FOR FACSIMILE DATA MODEM SIGNALS
SYSTEME DE TRANSMISSION SECURISEE POUR SIGNAUX MODEM DE DONNEES DE TELECOPIE

Patent Applicant/Assignee:
AMIK INC, 10580 S.W. McDonald Street, Suite 202, Tigard, OR 97224, US, US (Residence), US (Nationality)
Inventor(s):
COLLETT Gordon C, 2155 N.W. Chrystal Drive, McMinnville, OR 97128, US
GALE Gary A, 47665 N.W. Deer Court, Box 5018, Manning, OR 97125, US
Legal Representative:
ROSENBERG Gerald B, 285 Hamilton Avenue, Suite 520, Palo Alto, CA 94301, US
Patent and Priority Information (Country, Number, Date):
Patent: WO 200067466 A1 20001109 (WO 0067466)
Application: WO 2000US11430 20000428 (PCT/WO US0011430)
Priority Application: US 99303505 19990430
Designated States: AU CA IN MX
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: **H04N-001/44**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9464

English Abstract
A security system operates to secure the transmission of data between authorized modems and against interception by an unauthorized modem. The modems each implement a defined protocol that includes negotiation and data transport portions of a communications session that is conducted over a network utilizing signals selectively occurring in a plurality of frequency channels. The security device includes a first interface coupleable to a modem to exchange first predetermined signals occurring in a first plurality of frequency channels and a second interface coupleable to a network to exchange second predetermined signals occurring in a second plurality of frequency channels. A signal processor is coupled between the first and second interfaces, to implement a bidirectional conversion of the signals between the first and second plurality of frequency channels by frequency shifting the first and second predetermined signals between the first and second pluralities of frequency channels. Further, the security device can provide for a first frequency shift of greater than a predetermined frequency tolerance specified by the defined protocol for a first portion of said communications session and a second frequency shift for a second portion of the communications session.

French Abstract
Cette invention se rapporte a un systeme de securite qui fonctionne de facon a securiser la transmission de donnees entre des modem autorises et de facon a empecher l'interception de ces donnees par un modem non autorise. Les modem appliquent chacun un protocole defini qui contient les parties negociation et transport de donnees d'une session de communication ouverte sur un reseau utilisant des signaux voyageant selectivement dans plusieurs canaux de frequences. Ce dispositif de securite utilise une premiere interface pouvant etre couplee a un modem pour l'echange d'un premier groupe de signaux predetermines voyageant dans un premier groupe de canaux de frequence et une seconde interface pouvant etre couplee a un reseau pour l'echange d'un second groupe de signaux predetermines voyageant dans un second groupe de canaux de frequences. Un processeur de signaux est couple entre les premiere et seconde interfaces, pour executer une conversion bidirectionnelle des signaux entre le premier et le second groupe des canaux de frequences par decalage de frequences des premiers et des seconds signaux predetermines

entre les premier et second groupes de canaux de frequences. Ce dispositif de securite peut en outre assurer un premier decalage de frequence d'une tolerance de frequence superieure a une tolerance de frequence predeterminee, specifiee par le protocole defini pour une premiere partie de la session de communication et un second decalage de frequence pour une seconde partie de la session de communication.

Legal Status (Type, Date, Text)
Publication 20001109 A1 With international search report.
Examination 20010607 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **H04N-001/44**
Fulltext Availability:
Detailed Description

Detailed Description
... security mode, or may operate in the clear or any available security mode; (3) a **low** -security encoding **key** ; and (4) a **high - security key** seed value. In alternate embodiments of the present 1 5 invention, the code selector 164...

...be supported in a preferred method of operation in accordance with the present invention. The **low - security** process path preferably uses a fixed security **key** , while the **high - security** process path includes a **key** exchange. In initial embodiments, the **high - security** device is not interoperable with **low - security** devices unless pre-preemptively set to emulate a low-security device by a manual switch...Also, the inquiry/response exchange may be expanded to allow for adaptive transitions between different **high** and **low - security** levels and, potentially, the use of different **key** exchange and permutation **algorithms** . Nonstandard DTMF tones, or other tones altogether, can also be utilized in the inquiry/response...
? t23/5,k/20

23/5,K/20 (Item 20 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00731720 **Image available**
ELECTRONIC ACCESS CONTROL SYSTEM AND METHOD
SYSTEME ET PROCEDE DE COMMANDE D'ACCES ELECTRONIQUE
Patent Applicant/Assignee:
INTERNATIONAL BUSINESS MACHINES CORPORATION, New Orchard Road, Armonk, NY 10504, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
GULCU Ceki, Rifertstrasse 16, CH-8134 Adliswil, CH, CH (Residence), CH (Nationality), (Designated only for: US)
Legal Representative:
KLETT Peter Michael, International Business Machines Corporation, Saumerstrasse 4, CH-8803 Ruschlikon, CH
Patent and Priority Information (Country, Number, Date):
Patent: WO 200045016 A1 20000803 (WO 0045016)
Application: WO 2000IB32 20000112 (PCT/WO IB0000032)
Priority Application: EP 99101806 19990128
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES

FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU
LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA
UG US UZ VN YU ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: E05B-049/00
International Patent Class: **H04L-009/32** ; G07C-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6910

English Abstract
Disclosed is a new and flexible approach for managing physical security in an electronic lock-and-key system. The novel approach does away with cabling or other direct connecting between locks (2) and a system management center. The (physical) keys (3) serve to disseminate access control and other information within the system in a snowball-like way, using an adapted, but simple networking protocol. Whenever appropriate, cryptographic schemes are applied to protect the system.

French Abstract
La presente invention concerne une nouvelle approche souple de gestion de la securite physique dans un systeme electronique a serrures et cles. Cette nouvelle approche supprime le cablage ou toute autre connexion directe entre des serrures (2) et un centre de gestion de systeme. Les cles (3) (physiques) servent a disseminer les informations de commande d'acces et d'autres informations dans le systeme selon un effet boule de neige, a l'aide d'un protocole de reseau adapte mais simple. Au besoin, des programmes cryptographiques sont appliques pour proteger le systeme.

Legal Status (Type, Date, Text)
Publication 20000803 A1 With international search report.

International Patent Class: **H04L-009/32** ...
Fulltext Availability:
Detailed Description

Detailed Description
... key versus public key based architecture it should have become clear that, because of the **key** explosion problem, a shared **key** architecture is suitable only for **low security** applications or for small scale deployment, whereas **high security** applications or universal deployment both mandate public **key** cryptography.

It should also have become clear that the invented flexible architecture for managing physical...

? t23/5,k/1-2,7,16-18

23/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01602761
Method and apparatus for securing digital assets
Verfahren und Vorrichtung zur Sicherung von digitalen Gutern
Procede et appareil de protection de biens numeriques
PATENT ASSIGNEE:
Pervasive Security Systems Inc., (4318190), 535 Middlefield Road, Suite No. 120, Menlo Park, California 94025, (US), (Applicant designated States: all)
INVENTOR:
Garcia, Denis Jacques Paul, 696 Towle Way, Apt. 33, Palo Alto, CA 94306, (US)
LEGAL REPRESENTATIVE:
Ablett, Graham Keith et al (53085), Ablett & Stebbing, Caparo House, 101-103 Baker Street, London W1U 6FQ, (GB)
PATENT (CC, No, Kind, Date): EP 1326157 A2 030709 (Basic)
EP 1326157 A3 031210
APPLICATION (CC, No, Date): EP 2002258536 021211;
PRIORITY (CC, No, Date): US 339634 P 011212; US 74804 020212; US 159537 020531
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO
INTERNATIONAL PATENT CLASS: **G06F-001/00**

ABSTRACT EP 1326157 A2
The present invention relates to digital assets which are in a secured form that only those with granted access rights can access. Even with the proper access privilege, when a secured file is classified, at least a security clearance key is needed to ensure those who have the right security clearance can ultimately access the contents in the classified secured file. According to one embodiment, a secured file or secured document includes two parts: a header, and an encrypted data portion. The header includes security information that points to or includes access rules, a protection key and a file key. The access rules facilitate restrictive access to the encrypted data portion and essentially determine who the secured document can be accessed. The file key is used to encrypt/decrypt the encrypted data portion and protected by the protection key. If the contents in the secured file are classified, the file key is jointly protected by the protection key as well as a security clearance key associated with a user attempting to access the secured file.
ABSTRACT WORD COUNT: 175
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 030709 A2 Published application without search report
Search Report: 031210 A3 Separate publication of the search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200328	1469
SPEC A	(English)	200328	9246
Total word count - document A			10715
Total word count - document B			0

Total word count - documents A + B 10715

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION the key generator 244 generates keys 246 of different lengths or forms, each of the **keys** 246 corresponds to a security level, such as level 1 (**highest security**), level 2, ..., level N (**lowest security**). In another embodiment, each of the **keys** 246 generated by the **key** generator 244 is embedded with a signature signifying a security level. Other methods of specifying...
...secured files classified in the same security level, it is preferable to permit a clearance **key** with a **higher security** level to access secured files classified in the **lower security** levels. In other words, a clearance **key** in level 1 (i.e., the **highest security** level primarily designated to secured files classified as "top secret") can be used to access...

23/5,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01310513
Optical disk
Optische Platte
Disque optique
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (1855503), 1006, Oaza Kadoma, Kadoma-shi, Osaka 571, (JP), (Applicant designated States: all)
INVENTOR:
Oshima, Mitsuaki, 115-3, Minamitatsumi-cho, Katsura, Nishikyo-ku, Kyoto-shi, Kyoto 615, (JP)
Gotoh, Yoshiho, Room 201, 9-17, Higashinakahama 4-chome, Jyoto-ku, Osaka-shi, Osaka 536, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1120777 A2 010801 (Basic)
EP 1120777 A3 011010
APPLICATION (CC, No, Date): EP 2001108949 951116;
PRIORITY (CC, No, Date): JP 94283415 941117; JP 9516153 950202; JP 95261247 951009
DESIGNATED STATES: DE; FR; GB
RELATED PARENT NUMBER(S) - PN (AN):
EP 741382 (EP 95938017)
INTERNATIONAL PATENT CLASS: G11B-020/00; **G06F-001/00** ; G11B-007/00; G11B-027/30; G11B-023/28; G11B-013/04; G11B-011/105; G11B-019/02; G11B-019/12; G11B-007/007; G11B-007/26; G11B-020/12; G11B-027/10

ABSTRACT EP 1120777 A2
The invention comprises:
an optical disk with an embossed data zone having pits and projections indicating data signals readable by light irradiation, and
a barcode pattern indicating information formed on said embossed data zone.
ABSTRACT WORD COUNT: 37
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Cette invention se rapporte a un support d'enregistrement dans lequel sont stockes un contenu de vente au detail et un contenu de superdistribution, lequel est crypte selon un systeme cryptographique de bloc. L'en-tete de superdistribution est attache au contenu de superdistribution et crypte en fonction d'un systeme cryptographique a cle publique. L'en-tete de superdistribution contient une cle de decryptage permettant de decrypter le systeme cryptographique de bloc. Le systeme cryptographique a cle publique se caracterise par l'utilisation d'un dispositif connecte a un reseau de communication pour le decryptage. Le decryptage est realise lorsque le support d'enregistrement est charge dans le dispositif en question, avec un prix a payer par l'intermediaire du reseau de communication.

Fulltext Availability:
Detailed Description

Detailed Description
... 56-bit encryption key and the DES algorithm.

Here, the RSA encryption algorithm is a **public key** system that provides **higher security** than the DES encryption algorithm which is a **common key** system. Encryption keys with higher bit numbers ensure **higher security** . In this way, a higher content grade is associated with an encryption key and an...

12/5,K/20 (Item 20 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00287563
SECRET KEY EXCHANGE
ECHANGE DE CODES SECRETS
Patent Applicant/Assignee:
LEIGHTON Frank Thomson,
MICALI Silvio,
Inventor(s):
LEIGHTON Frank Thomson,
MICALI Silvio,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9505712 A2 19950223
Application: WO 94US9103 19940812 (PCT/WO US9409103)
Priority Application: US 93106932 19930813
Designated States: CA AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE
Main International Patent Class: H04L-009/30
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7517

English Abstract
The present invention describes a method for enabling users of a cryptosystem to agree on secret keys. In one embodiment, a trusted agent chooses at least one individual key for each user, with at least a portion of such individual key being secret. At least some of the individual keys are then stored in physically secure devices, and the pair of users i and j use their individual keys to compute a common secret key. In another embodiment, each trustee of a group of trustees chooses at least one individual key for each user, with at least some portion of such individual key being secret. The keys chosen by a

sufficiently small number of such trustees, however, are insufficient for computing the common secret key of the users. Other hardware and software key exchange protocols based on these two techniques are also disclosed.

French Abstract

L'invention porte sur un procede permettant aux usagers d'un cryptosysteme de se mettre d'accord sur des codes secrets. Dans l'une des realisations, un homme de confiance choisit un code pour chacun des usagers, dont au moins une partie est tenue secrete. Au moins certains de ces codes individuels sont deposes dans des dispositifs proteges. Les usagers i and j utilisent alors leurs codes respectifs pour calculer un code secret commun. Dans une autre realisation, chacun des membres d'un groupe d'hommes de confiance choisit au moins un code pour chacun des usagers dont au moins une partie est tenue secrete. Neanmoins, les codes choisis par un nombre suffisamment fiable de ces hommes de confiance sont insuffisants pour calculer le code secret commun des usagers. Sont egalement exposes d'autres protocoles d'echange de codes bases sur ces deux techniques aussi bien au niveau du materiel que des logiciels.

Fulltext Availability:
Claims

Claim
... having a pair of users i and j use their individual keys to compute a **common secret key** .

2. The method as described in Claim 1 wherein some of the users belong to the individual keys of users of **lower security** levels contain substantially no useful information for computing the **common secret key** of a pair of users of **higher security** levels.

4. A method for enabling users of a cryptosystem to agree on **secret keys** , comprising the
steps of:
for each user, having each trustee Pound Sterling of a group...
...chosen by a sufficiently small 30 number of trustees are substantially insufficient for computing the **common** secret key of the ...of a lower security level contain substantially no useful information for computing the common secret **key** of a pair of users of a higher 10 ...any subgroup of users of a lower security level are not useful for computing the **common secret key** of a pair of honest users of a higher security levels.

8. A method for enabling users of a cryptosystem to agree on **secret keys** , comprising the
steps of:
generating at least one **public key** for each user by interating at least a conventional one-way function on at least one secret value; and having a **common secret key** for a pair of users 25 be computable based on information that includes one user's secret information and the other's **public key** .

9. The method as described in Claim 8 wherein some ofthe users belong to different...

...The method as described in Claim 9 wherein secret information relative to users of a **lower security** level is substantially useless for computing the **common secret key** of a pair of users of a **higher security** level.
SUBSTITUTE SHIFT (ftU 2$

11. A method, using secure chips, for enabling users of t of a group of trustees 5 generate at least one **public key** for each user by evaluating at least one conventional one-way function on at **least** one **secret** value; having a **common secret key** for a pair of users be computable based on information that includes 10 secret information...12 wherein any secret information relative to a sufficiently small group of users of a **lower** security level is substantially useless for computing the common **secret key** of a pair of users of a higher **security** level.

14. A method for enabling users of a cryptosystem to agree on **secret keys** , comprising the
steps of:
generating at least one **public key** for each pair of users; and
having a **common secret key** for a pair of users be computable based on information that includes 35 their own **public key** and their own **secret keys** .
SUBSTITUTE SHEET (RULE 26)
15. A method for enabling users of a cryptosystem to agree on **secret** keys, comprising the steps of:
generating at least one **common public key** for 5 each pair of users; and
generating at least one **secret key** per user; and having a **common secret key** for a pair of users be computable based on information that includes the **common public key** for the pair of users and the 10 **secret keys** of the pair of users.

16. A method for enabling ...relative to that user generated by the trustees, a piece of information that includes at **least** one secret key and wherein the pieces of information generated by a sufficiently small number of trustees are practically insufficient to compute the common secret **key** of a pair of users.;
generating at least one **common public key** for a pair of users; and
having a **common secret key** for a pair of users be computable based on information that includes the **common public key** for the pair of users and the **secret keys** of the pair of users.
35
SUBSTITUTE SHEET (RULE 26)
?